RESEARCH PROJECT REGARDING PAYMENT SERVICES, BANK GROUP REGULATIONS AND OTHERS

FOR

JAPAN FINANCIAL SERVICES AGENCY

FINAL REPORT - EUROPE

30 MARCH 2015

BAKER & McKENZIE

1428773-v2\TOKDMS

Table of Contents

1428773-v2\TOKDMS

PAYMENT SERVICES - EUROPEAN UNION

1. Assignment

This memorandum responds to the questions of the document provided to us dated 9 December 2014, entitled "*Guidance for research on payment services-related matters (Europe)*". This document is a questionnaire relating to the regulation of certain financial services in the European Union, focussing on payment services and the issuing of e-money in particular.

This assignment is carried out by Baker&McKenzie's London office, Frankfurt office and Antwerp office, under the global supervision and coordination of the Tokyo office. It is envisaged that the London office responds to the questionnaire from a UK law perspective, the Frankfurt office from a German law perspective and the Antwerp office from a general European Union law perspective.

2. Scope

The scope of this memorandum is limited to payment-related general European Union law only and will not elaborate on national laws of the individual Member States of the European Union. The scope of this memorandum will, as a general rule, be limited to the regulatory framework of the European Union on payment services and e-money.

This memorandum will not elaborate on European Union law related to the regulation of financial institutions other than payment institutions and e-money institutions. E.g., the regulation of credit institutions is excluded from the scope of this directive. In addition, this memorandum does only discuss payment services and e-money regulations. It does not describe other bank services regulations or other specific regulations (such as debt collection regulations).

This memorandum is limited to "research 1" of the questionnaire. "Research 2" and "research 3" of the questionnaire are excluded from the scope of this memorandum and are only to be looked at from a UK and German law perspective (by the London office and Frankfurt office respectively).

Section 3 of this memorandum analyses and qualifies the Japanese payment-related services - as identified in the questionnaire - under EU law, section 4 provides a high-level overview of the EU legal framework on payment services and section 5 provides an overview of possible, future changes to that legal framework.

We have responded to these questions to the degree permitted by the budgetary constraints specified by the J-FSA, and therefore this memorandum is not necessarily exhaustive. We have attempted to provide as much relevant information as possible within the specified budgetary constraints. Accordingly, our response is necessarily general in nature. We have noted in the body of this memorandum areas that may require further research. In those instances, we would be pleased to discuss further with you whether it would be helpful to explore those areas further and our estimate of how much it would cost to do so.

3. Qualification of the Japanese payment and settlement services under EU law

3.1 General overview of the scope of application of the Payment Services Directive

(a) Material scope

Directive 2007/64/EC of the European Parliament and the Council of 13 November 2007 *on payment services in the internal market* (hereinafter ***the Payment Services Directive***) applies to payment services provided in the European Union.

The central definition of the Payment Services Directive is the definition of "payment service".

Article 4 (3) of the Payment Services Directive defines "payment service" as "*any business activity listed in the Annex*".

The Annex of the Payment Services Directive lists the following services as payment services:

- Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account

This service encompasses the service of placing money on a payment account.

Example: placement of money on a payment account by depositing money in an ATM machine or at the counter of a local bank.

- Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.

This service is the equivalent counterpart of the service listed under the first bullet. It envisages cash withdrawals at ATM machines or at the counter of a local bank.

- Execution of payment transactions, including transfers of funds on a payment account with the user's payment service provider or with another payment service provider:
    - execution of direct debits, including one-off direct debits,
    - execution of payment transactions through a payment card or a similar device,
    - execution of credit transfers, including standing orders.

According to article 4(5) of the Payment Services Directive, a payment transaction means an act, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.

The service includes:

- execution of direct debits. Article 4(28) of the Payment Services Directive defines ‘direct debit’ as a payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider. Example: direct debits are most commonly used to pay invoices of utilities companies (electricity, gas, telecom, etc.).
- execution of payment transactions through a payment card or a similar device. The Payment Services Directive does not define a payment card. It includes, at least, debit, credit and e-money cards.
- execution of credit transfers, including standing orders. This encompasses the service of wiring money from one account to another. Standing orders are automatic credit transfers, allowing the payer to wire money to a payee at fixed intervals. Example: standing orders are commonly used to pay rent.

    (i) Execution of payment transactions where the funds are covered by a credit line for a payment service user:

- execution of direct debits, including one-off direct debits,
- execution of payment transactions through a payment card or a similar device,
- execution of credit transfers, including standing orders.

The relevance of this service is rather limited since it is very similar to the service described under (c).

Example: the wiring of money in combination with the establishment of an overdraft facility, allowing the payment service user to use or withdraw more money than it has on its account, leading to a negative balance.

(ii) Issuing and/or acquiring of payment instruments

According to article 4(23) of the Payment Services Directive a 'payment instrument' means any personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used by the payment service user in order to initiate a payment order.

The definition of a payment instrument is very broad and ranges from payment cards and electronic lunch or service vouchers to even mobile phones that are being used to execute payments.

The issuer of the payment instrument is the payment service provider having a contractual relationship with the holder of the payment instrument. This is usually a credit institution that issued a payment card to a cardholder.

The acquirer of the payment instrument is the payment service provider having a contractual relationship with the merchant that accepts payment of the issued payment instrument in question. The acquirer is the credit or financial institution that processes card payments on behalf of a merchant. The place where such payments can be made are most commonly referred to as POS or Point of Sale. In practice the acquirer provides the merchant with a terminal that allows clients to pay by card for products or services of the merchant.

(iii) Money remittance

According to article 4(13) of the Payment Services Directive 'money remittance' means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

Money remittance is a simple payment service that is usually based on cash provided by a payer to a payment service provider, which remits the corresponding amount, for example via communication network, to a payee or to another payment service provider acting on behalf of the payee.

In some Member States supermarkets, merchants and other retailers provide to the public a corresponding service enabling the payment of utility and other regular household bills. Those bill-paying services should be treated as money remittance, unless the competent authorities consider the activity to fall under another payment service listed in the Annex.

A well-known institution that is commonly involved in the business of money transfer is Western Union.

(iv) Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services.

The intention of the European legislator with this provision was to bring mobile payments within the scope of the Payment Services Directive.

(b) Personal scope

The Payment Services Directive applies when a payment service provider provides a payment service to a payment service user.

(i) Payment service user

According to article 4(10) of the Payment Services Directive, 'Payment service user' means a natural or legal person making use of a payment service in the capacity of either payer or payee, or both.

Both payer and payee are defined by the Payment Services Directive. Article 5(7) of the Payment Services Directive defines ‘payer’ as a natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order. Article 5(8) of the Payment Services Directive defines ‘payee’ as a natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction.

These definitions are very broad and include private individuals and legal entities, acting as a consumer or a professional.

Where the payment service user is not a consumer, the parties may agree that certain provisions of the Payment Services Directive shall not apply, in whole or in part ("opt-out"). These provisions that can be opt-out of relate to information obligations, liability for non-authorized payment transactions and the execution of payment transactions. Consumers cannot opt-out from any provision of the Payment Services Directive.

Article 4(11) of the Payment Services Directive defines 'consumer' as a natural person who, in payment service contracts covered by the Payment Services Directive, is acting for purposes other than his trade, business or profession.

(ii) Payment service provider

Article 4(9) of the Payment Services Directive defines ‘payment service provider’ by referring to the bodies in article 1(1) of the Payment Services Directive and the legal and natural persons benefiting from the waiver under article 26 of the Payment Services Directive.

According to article 1(1) of the Payment Services Directive, Member States shall distinguish the following six categories of payment service providers:

- credit institutions within the meaning of article 4.1(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms (hereinafter CRR);
- electronic money institutions within the meaning of article 2(1)(a) of Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions (hereinafter e-money Directive);
- post office giro institutions which are entitled under national law to provide payment services;
- payment institutions within the meaning of the Payment Services Directive;
- the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities; and
- Member States or their regional or local authorities when not acting in their capacity as public authorities.

The application of the Payment Services Directive is confined to payment service providers whose main activity consists in the provision of payment services to payment service users. Such position is also confirmed in question no. 125 of the Payment Services Directive Questions & Answers stating that the rules apply to the provision of payment services as a regular occupation or business activity.

(c) Territorial scope

The Payment Services Directive shall apply to payment services provided within the European Union. However, with the exception of article 73 of the Payment Services Directive, Titles III and IV shall apply only where both the payer's payment service provider and the payee's payment service provider are, or the sole payment service provider in the payment transaction is, located in the European Union. Titles III and IV of the Payment Services Directive respectively relate to "transparency of conditions and information requirements for payment services" and "rights and obligations in relation to the provision of payment services".

(d) Negative scope

The Payment Services Directive shall not apply to any of the following (notwithstanding the fact that other European or local regulations may apply hereto):

- payment transactions made exclusively in cash directly from the payer to the payee, without any intermediary intervention;
- payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee;
- professional physical transport of banknotes and coins, including their collection, processing and delivery;
- payment transactions consisting of the non-professional cash collection and delivery within the framework of a non-profit or charitable activity;
- services where cash is provided by the payee to the payer as part of a payment transaction following an explicit request by the payment service user just before the execution of the payment transaction through a payment for the purchase of goods or services;
- money exchange business, that is to say, cash-to-cash operations, where the funds are not held on a payment account;
- payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee:
    - ➢ paper cheques in accordance with the Geneva Convention of 19 March 1931 providing a uniform law for cheques;
    - ➢ paper cheques similar to those referred to in point (i) and governed by the laws of Member States which are not party to the Geneva Convention of 19 March 1931 providing a uniform law for cheques;
    - ➢ paper-based drafts in accordance with the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;
    - ➢ paper-based drafts similar to those referred to in point (iii) and governed by the laws of Member States which are not party to the Geneva Convention of 7 June 1930 providing a uniform law for bills of exchange and promissory notes;
    - ➢ paper-based vouchers;
    - ➢ paper-based traveller's cheques; or
    - ➢ paper-based postal money orders as defined by the Universal Postal Union;

- payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses and/or central banks and other participants of the system, and payment service providers, without prejudice to article 28 of the Payment Services Directive;

- payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in point (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services and any other entities allowed to have the custody of financial instruments;

- services provided by technical service providers, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, including processing and storage of data, trust and privacy protection services, data and entity authentication, information technology (IT) and communication network provision, provision and maintenance of terminals and devices used for payment services;

- services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services;

- payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services;

- payment transactions carried out between payment service providers, their agents or branches for their own account;

- payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group; or

- services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not a party to the framework contract with the customer withdrawing money from a payment account, on condition that these providers do not conduct other payment services as listed in the Annex of the Payment Services Directive.

3.2 General overview of the scope of application of the e-money directive

(a) Material scope

The e-money Directive lays down the rules for the pursuit of the activity of issuing electronic money in the European Union.

According to article 2(2) of the e-money Directive, ‘electronic money’ means electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of article 4 of the Payment Services Directive, and which is accepted by a natural or legal person other than the electronic money issuer.

An example of software-based e-money is PayPal. PayPal is an American, international digital wallet based e-commerce business allowing payments and money transfers to be made through the Internet. In Belgium, Proton is an example of hardware-based e-money (money is stored on the chip of a bank card). Proton will cease to operate as of January 2015 however. In Germany, the most prominent example of a card with an e-money function is the “GeldKarte” which has been developed by the German banking industry.

(b) Personal and territorial scope

The e-money Directive applies to e-money issuers.

According to article 2(3) of the e-money Directive, ‘electronic money issuer’ means entities referred to in article 1(1) of the e-money Directive, institutions benefiting from the waiver under article 1(3) of the e-money Directive and legal persons benefiting from a waiver under article 9 of the e-money Directive.

According to article 1(1) of the e-money Directive, the Member States shall recognise the following categories of electronic money issuer:

- credit institutions as defined in point 1 of article 4 CRR including, in accordance with national law, a branch thereof, where such a branch is located within the European Union and its head office is located outside the European Union;
- electronic money institutions as defined in point 1 of article 2 of the e-money Directive including, in accordance with article 8 of the e-money Directive and national law, a branch thereof, where such a branch is located within the European Union and its head office is located outside the European Union;
- post office giro institutions which are entitled under national law to issue electronic money;
- the European Central Bank and national central banks when not acting in their capacity as monetary authority or other public authorities;
- Member States or their regional or local authorities when acting in their capacity as public authorities.

3.3 Existence and qualification of the Japanese payment services listed in the questionnaire under EU law

(a) Exchange transactions by banks or funds transfer service providers

Based on the exhibit you provided us with, we understand that exchange transactions by banks or funds transfer service providers encompasses the service whereby funds are being transferred from one person to another without direct (physical) cash delivery between the persons involved.

Such a service would qualify as the payment service "money remittance" under the Payment Services Directive, triggering licensing requirements.

(b) Prepaid payment instruments

Based on the exhibit you provided us with, we understand that a distinction is being made between six different types of prepaid payment instruments: self-provided instruments, third party-provided instruments, paper-based instruments, IC chip-based instruments, server-based instruments and post-paid instruments.

(i) Self-provided instruments

We understand that the self-provided instrument can only be used in one particular shop or store and that the instrument is directly issued by the merchant in question who sells the products or provides the services. An example would be a Starbucks Card, issued by Starbucks and only to be used in Starbucks.

Under EU law, such an instrument would not qualify as e-money under the e-money Directive. In order to qualify as e-money, the payment instrument must be accepted by a natural or legal person other than the electronic money issuer.

Self-provided instruments are not accepted by a natural or legal person other than the electronic money issuer and do not constitute e-money. No licensing requirements under the e-money Directive will be triggered.

(ii) Third party-provided instruments

We understand that third party-provided instruments are issued by a third party who does not sell own products or services but acts as the intermediary between the user of the instrument and the seller. This includes gift vouchers and gift certificates that can be used in various shops (e.g., Book Gift Card in Japan can be used in almost all book shops in Japan to buy books).

According to article 1(4) of the e-money Directive in conjunction with article 3(k) of the Payment Services Directive, the e-money Directive does not apply to monetary value stored on specific pre-paid instruments, designed to only be used within a limited network. However, these specific instruments enter within the scope of the e-money Directive if they develop, as stated in recital (5), into general-purpose instruments "designed for a network of service providers which is continuously growing".

The e-money Directive does not apply to monetary value stored on specific pre-paid instruments, designed to address precise needs that can be used only in a limited way, because they allow the electronic money holder to purchase goods or services only in the premises of the electronic money issuer or within a limited network of service providers under direct commercial agreement with a professional issuer, or because they can be used only to acquire a limited range of goods or services.

An instrument should be considered to be used within such a limited network if it can be used only either for the purchase of goods and services in a specific store or chain of stores, or for a limited range of goods or services, regardless of the geographical location of the point of sale. Such instruments could include store cards, petrol cards, membership cards, public transport cards, meal vouchers or vouchers for services (such as vouchers for childcare, or vouchers for social or services schemes which subsidise the employment of staff to carry out household tasks such as cleaning, ironing or gardening), which are sometimes subject to a specific tax or labour legal framework designed to promote the use of such instruments to meet the objectives laid down in social legislation.

Where such a specific-purpose instrument turns into or becomes a general-purpose instrument, the exemption from the scope of the e-money Directive no longer applies. Instruments which can be used for purchases in stores of listed merchants are not exempted from the scope of the e-money Directive as such instruments are typically designed for a network of service providers which is continuously growing.

We do not know what the situation is with regard to the Book Gift Card you refer to. It is for the national authorities to analyse and decide based on the business models used if the issuer of these gift vouchers can be excluded or not from the application of the e-money Directive, and thus whether or not the issuer requires a licence to engage in such activity.

(iii) Paper-based instruments

We understand that paper-based instruments are paper-based certificates containing monetary value.

Under the assumption that no monetary value is being electronically, including magnetically, stored on a device, paper-based instruments do not constitute e-money.

For the avoidance of doubt, paper-based vouchers are also explicitly excluded from the scope of the Payment Services Directive.

(iv) IC chip-based instruments

We understand that IC chip-based instruments are instruments in which the value is recorded on the integrated circuit (IC) chip embedded in devices, such as plastic cards and mobile phones, etc.

Under the assumption that monetary value is being stored electronically on the IC chip on receipt of funds for the purpose of making payment transactions as defined in point 5 of article 4 of the Payment Services Directive, and which is accepted by a natural or legal person other than the electronic money issuer, IC chip-based instruments constitute e-money. The issuer of such IC chip-based instruments must be licensed to engage in such an activity.

(v) Server-based instruments

We understand that with server-based instruments monetary value is recorded and managed centrally on the computer server of the issuer of the instrument. The monetary value is not recorded on a physical medium, such as a document or a card. Server-based instruments are designed for use on the Internet. Examples of such server-based instruments are Amazon gift certificates. The most well-known and successful example of server based e-money is PayPal.

As a general rule, monetary value stored on a server which is issued on receipt of funds for the purpose of making payment transactions as defined in point 5 of article 4 of the Payment Services Directive, and which is accepted by a natural or legal person other than the electronic money issuer, constitutes e-money. The absence of a physical medium to story the monetary value on is irrelevant.

Recital 8 of the e-money Directive stipulates that the definition of electronic money covers electronic money whether it is held on a payment device in the electronic money holder’s possession or stored remotely at a server and managed by the electronic money holder through a specific account for electronic money. The definition of e-money is kept intentionally broad to avoid hampering technological innovation and to cover not only all the electronic money products available today in the market but also those products which could be developed in the future.

As far as your example on Amazon gift certificates concerns, however, we refer to our comments on third-party provided instruments:

According to article 1(4) of the e-money Directive in conjunction with article 3(k) of the Payment Services Directive, the e-money Directive does not apply to monetary value stored on instruments, designed to only be used within a limited network. However, these specific instruments enter within the scope of the e-money Directive if they develop, as stated in recital (5), into general-purpose instruments "designed for a network of service providers which is continuously growing".

We do not know what the situation is with regard to the Amazon gift certificates you refer to. It is for the national authorities to analyse and decide based on the business models used if the issuer of these gift vouchers can be excluded or not from the application of the e-money Directive, and thus whether or not the issuer requires a licence to engage in such activity.

(vi) Post-paid instruments

We understand that post-paid instruments are payment instruments under which the issuers provide credit to the users, and the users shall repay the credit to the issuer afterwards.

We do not believe that post-paid instruments constitute e-money due to the fact that no money is being stored on a device (no storage of money). Accordingly, the issuing of post-paid instruments will not require a license as an e-money institution.

The issuing of such a payment instrument will, however, qualify as a payment service within the meaning of the Payment Services Directive (payment service referred to in point 5 of the Annex:

"issuing of payment instruments"). Engaging in such an activity will require a license as a payment institution.

The Payment Services Directive regulates the granting of credit by payment institutions, i.e. the granting of credit lines and the issuance of credit cards, only where it is closely linked to payment services. Only if credit is granted in order to facilitate payment services and such credit is of a short-term nature and is granted for a period not exceeding twelve months, including on a revolving basis, it is allowed for payment institutions to grant such credit with regard to their cross-border activities, on condition that it is refinanced using mainly the payment institution's own funds, as well as other funds from the capital markets, but not the funds held on behalf of clients for payment services.

Article 16(3) of the Payment Services Directive stipulates that payment institutions may grant credit related to payment services referred to in points 4, 5 or 7 of the Annex to the Payment Services Directive (please refer to section 1.1 (a) of this memorandum for the content of such payment services), where the conditions laid down in article 16(3) and (5) of the Payment Services Directive are met.

This means that e-money institutions may grant credit related to payment services referred to in points 4, 5 or 7 of the Annex only if the following conditions are met:

- the credit shall be ancillary and granted exclusively in connection with the execution of a payment transaction;
- notwithstanding national rules on providing credit by credit cards, the credit granted in connection with a payment and executed in accordance with article 10(9) and article 25 of the Payment Services Directive shall be repaid within a short period which shall in no case exceed twelve months;
- such credit shall not be granted from the funds received or held for the purpose of executing a payment transaction; and
- the own funds of the payment institution shall at all times and to the satisfaction of the supervisory authorities be appropriate in view of the overall amount of credit granted.

The above is without prejudice to Directive 2008/48/EC of the European Parliament and the Council of 23 April 2008 *on credit agreements for consumers* (hereinafter ***the Consumer Credit Directive***) or any other relevant European Union or national legislation regarding conditions for granting credit to consumers not harmonised by European Union law. The Consumer Credit Directive imposes certain information obligations to the creditor and grants certain rights to the consumer-debtor such as the right of early repayment.

As a general rule, the activity of issuing post-paid instruments will require a license as a payment institution under the Payment Services Directive. The issuing of such payment instruments may also trigger application of the Consumer Credit Directive.

Note, however, that the Consumer Credit Directive does not apply to credit agreements where the credit is granted free of interest and without any other charges and credit agreements under the terms of which the credit has to be repaid within three months and only insignificant charges are payable. This exemption might be relevant for the issuing of post-paid instruments (note that other exemptions to the Consumer Credit Directive are listed under article 2(2) of that same directive).

(c) Post-pay e-money

We assume that post-pay e-money is similar to post-paid instruments. Accordingly, we refer to our comments above. The issuer will be subject to licensing requirements.

(d) Payment receiving agency or collection agency

We understand that a payment receiving agency (or a collection agency) is, for example, generally used for the payment of utilities (such as electric/gas utility expense etc.) in Japan. In this scheme, the users pay the fees for utilities, telephone service charges etc. at the corner stores (tobacco shop/kiosk/supermarket) widely spread in the country. Such agency collects the payment from payers in favour of the recipient who is the user of this service, and transfers the collected amount to the recipient.

Under the Payment Services Directive, a bill payment service qualifies as money remittance, which is a payment service under the Payment Services Directive.

Money remittance is a simple payment service that is usually based on cash provided by a payer to a payment service provider, which remits the corresponding amount, for example via communication network, to a payee or to another payment service provider acting on behalf of the payee.

In some Member States supermarkets, merchants and other retailers provide to the public a corresponding service enabling the payment of utility and other regular household bills. Those bill-paying services should be treated as money remittance as defined in the Payment Services Directive, unless the competent authorities consider the activity to fall under another payment service listed in the Annex.

While some business models for bill paying services clearly fall within the scope of the Payment Services Directive (e.g. when the service is being provided by the bill payment service provider to the customer wishing to pay his invoice and is effectively a simple money remittance service), other models operate on the basis of the invoice issuer as the principal, with the provider as his agent providing a means by which the bill payer can settle its bills. In this model, the invoice issuer provides the consumer with the option of settling the invoice by payment to the bill payment service provider. Such payment extinguishes the debt by virtue of the agency relationship between the bill payment service provider and the invoice issuer and is therefore equivalent to direct payment to the invoice issuer. In the event of the failure of the bill payment service provider, the risk lies with the invoice issuer. The bill payer has no exposure, as the receipt issued by the bill payment service provider is evidence of the debt having been extinguished. This is not a payment service; because the invoice is settled as soon as the money is given to the bill payment service provider, there is no request for execution of a payment transaction and therefore no payment order being made. This service would therefore fall under the exemption of article 3(b) of the Payment Services Directive.

If the service qualifies as money remittance, licensing requirements will be triggered. If the service benefits from the exemption of article 3(b) of the Payment Services Directive, no licensing requirements will be triggered.

Some countries have (consumer) debt collection regulations.

(e) Cash-on-delivery

We understand that cash-on-delivery is a service whereby a courier receives payment from a recipient in exchange for delivery of goods. Next, the courier transfers the received amounts to the sender of the goods.

The scope of this service and the nature of the underlying contractual relations between the parties involved are unclear to us. Depending on the exact circumstances and nature of the service, this service can either qualify as the physical transportation of banknotes and coins or as some sort of an invoice agency model:

(i) Physical transportation of banknotes and coins

The Payment Services Directive does not apply to the professional physical transport of banknotes and coins, including their collection, processing and delivery. It might be argued that cash-on-delivery is excluded from the Payment Services Directive, therefore not requiring a license to engage in such an activity.

Companies such as G4S which are specialized in the secured physical transportation of banknotes and coins fall outside the scope of the Payment Services Directive by virtue of article 3 (c) of the Payment Services Directive and do not require a license as a payment service provider.

(ii) Invoice agency model

In this model, the invoice issuer provides the consumer with the option of settling the invoice by payment to the bill payment service provider. Such payment extinguishes the debt by virtue of the agency relationship between the bill payment service provider and the invoice issuer and is therefore equivalent to direct payment to the invoice issuer. In the event of the failure of the bill payment service provider, the risk lies with the invoice issuer, as the client. The bill payer has no exposure, as the receipt issued by the bill payment service provider is evidence of the debt having been extinguished. This is not a payment service; because the invoice is settled as soon as the money is given to the bill payment service provider, there is no request for execution of a payment transaction and therefore no payment order being made. This service would therefore fall under the exemption of article 3 (b) of the Payment Services Directive. No licensing requirements will be triggered.

Some countries have (consumer) debt collection regulations.

(f) Account transfer agency

We understand that the service of an account transfer agency consists of the collection of fees for continuous services such as mobile phone charges, house rent etc. The account transfer agency receives the fee via bank transfer from the payer's bank account, and the agency transfers the collected amount to the recipient.

By using this service, the recipient can collect the fees (i.e. the mobile phone charge in case the recipient is a mobile phone service provider, and the house rent in case it is a landlord) from multiple payers every month/year through such agency, without making any direct requests to the payers to transfer their debt. In this way, this scheme can reduce the cost incurred by the recipient.

The same legal analysis of "Payment receiving agency or collection agency" (see above) would apply to this type of service: bill payment services qualify as money remittance. In case there is an agency relationship between the bill payment service provider and the invoice issuer, the service would fall under the exemption of article 3 (b) of the Payment Services Directive.

(g) Fund transfer agency

We understand that a fund transfer agency is an agent that transfers a specific amount of money to a designated bank account of a payee, on behalf of the payer.

For example, an employer, as a payer, may use this service to pay the monthly pay check of its employees.

The payer instructs the fund transfer agency to wire the money to the bank account(s) owned by the recipient (for example, the employees). Such instructions may be made in the form of a spread sheet or any other form accepted by the agency. The payer deposits the money in a bank account of the agency. Then, the agency transfers the money from its own bank account to the recipient's bank account as instructed by the payer.

This service would qualify as money remittance, which is a payment service under the Payment Services Directive. Engaging is such an activity will trigger licensing requirements.

According to article 4(13) of the Payment Services Directive ‘money remittance’ means a payment service where funds are received from a payer, without any payment accounts being created in the name of the payer or the payee, for the sole purpose of transferring a corresponding amount to a payee or to another payment service provider acting on behalf of the payee, and/or where such funds are received on behalf of and made available to the payee.

(h) Escrow services

We understand that an escrow service is an arrangement in which a trusted third party receives and disburses money or documents for the transacting parties in a transaction. In this arrangement the disbursement shall be made by the agent depending on the conditions agreed by the transacting parties.

Contrary to point-of-sale transactions, remote transactions imply by definition a time interval between payment and delivery of goods, and hence, create a conflict of interest between buyer and seller. Neither party is interested in transferring its assets (be it money or goods), before receiving the other party's agreed asset. This conflict is especially pertinent in an online context, where the remote nature of transactions is often accompanied by unknown or anonymous trade partners, which aggravates the lack of trust between trade partners.

An example of an escrow service provider is escrow.com, which is eBay's approved escrow service. Local escrow service examples include Pay&Deliver in Belgium, PayDutch in the Netherlands and Iloxx in Germany.

Online escrow services may be subject to the Payment Services Directive, depending on their underlying transaction scheme. As a general rule, escrow services are part of payment service 3 of the Annex, which consists of the execution of payment transactions.

If, however, the trusted third party operates as a mere escrow agent, its services shall not be considered as payment services. For example, in the Pay&Deliver scheme, the buyer's payment is transferred to an account which is administered by a third party, legally independent from Pay&Deliver. Hence, the payment is not executed by Pay&Deliver. However, if the trusted third party actually effects the payment, such service will be qualified as a payment service as defined in the Payment Services Directive. Consequently, the trusted third party will be considered as a payment institution, and shall be subject to the authorisation requirements as set out in the Payment Services Directive.

It should be noted that, if the escrow agent receives money on its own accounts, it might be considered as a deposit-taking business, which requires a license as a credit institution. According to article 16(4) of the Payment Services Directive, payment institutions are not allowed to engage in the business of taking deposits or other repayable funds from the public within the meaning of article 4(1) of Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 *on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012* (hereinafter ***CRR***).

(i) Credit card settlements

(i) issuing

Issuing means that a credit card company issues a credit card to a person approved to become a member upon credit examination of such person.

Issuing of payment instruments is expressly included in the Annex to the Payment Services Directive as constituting a payment service. Engaging in such an activity will require a license under the Payment Services Directive.

(ii) acquiring

Acquiring means that a credit card company authorizes a seller of goods or services as a participating merchant upon examination.

Acquiring of payment instruments is expressly included in the Annex to the Payment Services Directive as constituting a payment service. Engaging in such an activity will require a license under the Payment Services Directive.

(iii) international credit card brand services

International credit card brand services means the business conducted by international credit card brands, such as VISA and Master Card, including management of the worldwide network of settlement services and establishment or supervision of an operational standard in relation to credit card transactions.

The operation of these payment systems does not constitute payment services as such and are not covered by the Payment Services Directive.

Note that international credit card brand services are subject to the rules on "oversight". National rules on oversight are based on article 127(2) of the Treaty on Functioning of the European Union (hereinafter ***TFEU***) and on the Statute of the European System of Central Banks and the European Central Bank (hereinafter ***the Statute***).

The TFEU and the Statute contain a number of provisions relating to “clearing and payment systems” and assigns oversight responsibilities to the Eurosystem, composed of the ECB and the national central banks (hereinafter ***NCBs***) of the euro area. According to the fourth indent of article 127(2) TFEU, as mirrored in article 3.1 of the Statute, one of the basic tasks of the Eurosystem is to "*promote the smooth operation of payment systems*". The means by which this task is assigned is specified in article 22 of the Statute, according to which “*the ECB and national central banks may provide facilities, and the ECB may make regulations, to ensure efficient and sound clearing and payment systems within the community and with other countries*”. Such regulations constitute the rules on oversight.

In addition, the oversight activities of some NCBs are carried out on the basis of national laws and regulations, which complement and, in some cases, duplicate the Eurosystem’s competence.

(j) Settlement agency

We understand that a settlement agency is generally used in relation to credit card payments whereby the agency acts as an intermediary between the credit card acquirer and the merchants. Merchants using this structure are typically small-sized businesses that are not able to pass the strict requirements imposed by the international credit card brands such as VISA, Master Card, etc., and they can not equip themselves with the machines and devices required by such international brands. The settlement agency acts as an intermediary and collectively enters into an agreement with credit card brands, and it allows those smaller merchants to have indirect access to large credit card brands. PayPal is a well-known example of a settlement agency in Japan.

The service of settlement agent would qualify as acquiring of payment instruments, and is therefore a Payment Service within the meaning of the Payment Services Directive. Engaging in such an activity will require a license under the Payment Services Directive.

If the settlement agent merely engages in "IT acquiring and processing" without managing any cash flows, no licensing requirements as a payment institution would be triggered. If the settlement agent also receives the cash flows, licensing requirements will likely be triggered.

Note that, in 2007, PayPal Europe was granted a Luxembourg banking license, which, under European Union law, allows it to conduct banking business throughout the EU ("passporting"). It is therefore regulated as a bank by Luxembourg's banking supervisory authority, the *Commission de*

Surveillance du Secteur Financier (CSSF). All of the company's European accounts were transferred to PayPal's bank in Luxembourg in July 2007. Prior to this move, PayPal had been registered in the United Kingdom as PayPal (Europe) Ltd, an entity which was licensed as an electronic money issuer with the UK's *Financial Services Authority* (FSA) from 2004. This ceased in 2007, when the company moved to Luxembourg. PayPal, as a licensed credit institution, is allowed to provide payment services such as acquiring.

4. EU payment and settlement related regulations

4.1 Background of the EU legislative framework on payment services

One of the main objectives of the European Union is to ensure the proper functioning of the internal market, of which payment services are an essential part.

The main objective of the European Union with regard to payment services is the creation of a Single Euro Payment Area (hereinafter ***SEPA***).

SEPA stands for a European Union payments integration initiative. With the introduction of the euro currency in 1999, the political drivers of the SEPA initiative - EU governments, the European Parliament, the European Commission and the European Central Bank (hereinafter ***the ECB***) - have focused on the integration of the euro payments market.

The goal is to make payments in euro and across Europe as fast, safe and efficient as national payments are today. Once SEPA has been completed, there will no longer be any distinction between national and cross-border euro payments: they will all be domestic. Therefore, standards are being drawn up for the whole SEPA area for the three main payment instruments: credit transfers, direct debits and card payments.

To achieve this goal, the EU co-legislators, i.e. the European Parliament and the Council of the EU representing EU Member States' governments, adopted several legislative acts designed to drive forward the integration of the euro payments market.

The legal framework of the SEPA project exists (mainly) of the following three legislative acts:

- the Payment Services Directive
- Regulation 260/2012 of the European Parliament and the Council of 14 March 2012 establishing technical and business requirements for credit transfers and direct debits in euro (hereinafter the SEPA Regulation)
- Regulation 924/2009 of the European Parliament and the Council of 16 September 2009 on cross-border payments in the Community

4.2 High-level overview of key EU payment related regulations

(a) Payment Services Directive

(i) Introduction

The Payment Services Directive provides the legal foundation for the creation of an EU-wide single market for payments. The Payment Services Directive aims at establishing a modern and comprehensive set of rules applicable to all payment services in the European Union. The target is to make cross-border payments as easy, efficient and secure as 'national' payments within a Member State. The Payment Services Directive also seeks to improve competition by opening up payment markets to new entrants, thus fostering greater efficiency and cost-reduction. At the same time the Directive provides the necessary legal platform for the Single Euro Payments Area (SEPA).

The Payment Services Directive was formally adopted by the Council and the European Parliament on 13 November 2007.

Note that EU directives are not directly applicable in the Member States of the European Union. A directive is a legislative act that sets out a goal that all Member States of the EU must achieve. However, it is up to the individual countries to decide how. A regulation, on the other hand, is a binding legislative act and is directly applicable in all Member States without any implementation needed. It must be applied in its entirety across the EU.

The deadline for implementation of the Payment Services Directive by the Member States was set at 1 November 2009.

(ii) Scope of application

For the scope of application of the Payment Services Directive, we refer to section 1.1 of this memorandum.

(iii) Public law aspects of the Payment Services Directive

(A) Licensing requirements

Payment institutions must obtain a license prior to providing payment services. Member States shall require undertakings other than those referred to in article 1(1)(a) to (c), (e) and (f) and other than legal or natural persons benefiting from a waiver under article 26, who intend to provide payment services, to obtain authorisation as a payment institution before commencing the provision of payment services. An authorisation shall only be granted to a legal person established in a Member State.

For authorisation as a payment institution, an application must be submitted to the competent authorities of the home Member State, together with the following:

- a programme of operations, setting out in particular the type of payment services envisaged;
- a business plan including a forecast budget calculation for the first three financial years which demonstrates that the applicant is able to employ the appropriate and proportionate systems, resources and procedures to operate soundly;
- evidence that the payment institution holds initial capital provided for in article 6 of the Payment Services Directive;
- for the payment institutions referred to in article 9(1) of the Payment Services Directive, a description of the measures taken for safeguarding payment service users' funds in accordance with article 9 of the Payment Services Directive;
- a description of the applicant's governance arrangements and internal control mechanisms, including administrative, risk management and accounting procedures, which demonstrates that these governance arrangements, control mechanisms and procedures are proportionate, appropriate, sound and adequate;
- a description of the internal control mechanisms which the applicant has established in order to comply with obligations in relation to money laundering and terrorist financing under Directive 2005/60/EC on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing and Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 on information on the payer accompanying transfers of funds;
- a description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of its participation in a national or international payment system;

- the identity of persons holding in the applicant, directly or indirectly, qualifying holdings within the meaning of article 4(11) of Directive 2006/48/EC relating to the taking up and pursuit of the business of credit institutions (which directive is now replaced by CRD IV and CRR), the size of their holdings and evidence of their suitability taking into account the need to ensure the sound and prudent management of a payment institution;
- the identity of directors and persons responsible for the management of the payment institution and, where relevant, persons responsible for the management of the payment services activities of the payment institution, as well as evidence that they are of good repute and possess appropriate knowledge and experience to perform payment services as determined by the home Member State of the payment institution;
- where applicable, the identity of statutory auditors and audit firms as defined in Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts;
- the applicant's legal status and articles of association;
- the address of the applicant's head office.

Within three months of receipt of an application or, should the application be incomplete, of all the information required for the decision, the competent authorities shall inform the applicant whether the authorisation has been granted or refused. Reasons shall be given whenever an authorisation is refused.

(B) Capital requirements

Member States shall require payment institutions to hold, at the time of authorisation, initial capital, comprised of the items defined in article 57(a) and (b) of Directive 2006/48/EC *relating to the taking up and pursuit of the business of credit institutions* (which directive is now replaced by CRD IV and CRR) as follows:

- where the payment institution provides only the payment service listed in point 6 of the Annex, its capital shall at no time be less than EUR 20 000;
- where the payment institution provides the payment service listed in point 7 of the Annex, its capital shall at no time be less than EUR 50 000; and
- where the payment institution provides any of the payment services listed in points 1 to 5 of the Annex, its capital shall at no time be less than EUR 125 000.

(C) Other prudential rules

Other prudential rules of the Payment Services Directive relate to: i) the safeguarding of funds of payment service users (prohibition to commingle own funds with those of payment service users), ii) the use of branches or agents to which activities are outsourced (notification requirement, restriction on the outsourcing of operational functions of payment services), iii) possibility to withdraw a license, iv) record keeping, etc.

We did not include a detailed description of these other prudential rules for the time being. Please let us know if you wish us to elaborate on such provisions in a more detailed way.

(D) Passporting regime

Once a payment service provider is licensed as a payment institution, it can rely on the EU passporting regime to provide its services in other Member States of the EU.

According to article 10(9) of the Payment Services Directive, an authorisation shall be valid in all Member States and shall allow the payment institution concerned to provide payment services throughout the European Union, either under the freedom to provide services or the freedom of establishment, provided that such services are covered by the authorisation.

This implies that, if a payment service provider has obtained a license as a payment institution in one Member State, it can passport its license into any other Member State of the European Union. It can either do so by establishing a branch or subsidiary in that Member State (freedom of establishment) or by providing its payment services to payment service users in that Member State on a cross-border basis without establishing a branch or subsidiary in that Member State (freedom to provide services).

Any authorised payment institution wishing to provide payment services for the first time in a Member State other than its home Member State, in exercise of the right of establishment or the freedom to provide services, shall so inform the competent authorities in its home Member State. Within one month of receiving that information, the competent authorities of the home Member State shall inform the competent authorities of the host Member State of the name and address of the payment institution, the names of those responsible for the management of the branch, its organisational structure and of the kind of payment services it intends to provide in the territory of the host Member State.

In order to carry out the controls and take the necessary steps provided for in article 21 of the Payment Services Directive in respect of the agent, branch or entity to which activities are outsourced of a payment institution located in the territory of another Member State, the competent authorities of the home Member State shall cooperate with the competent authorities of the host Member State.

By way of cooperation, the competent authorities of the home Member State shall notify the competent authorities of the host Member State whenever they intend to carry out an on-site inspection in the territory of the latter. However, if they so wish, the competent authorities of the home Member State may delegate to the competent authorities of the host Member State the task of carrying out on-site inspections of the institution concerned.

The competent authorities shall provide each other with all essential and/or relevant information, in particular in the case of infringements or suspected infringements by an agent, a branch or an entity to which activities are outsourced. In this regard, the competent authorities shall communicate, upon request, all relevant information and, on their own initiative, all essential information.

The European Commission has published on its website more detailed and practical guidelines on Payment Services Directive passport notifications. These guidelines include, among others, standard notification forms and lists of national competent authorities.

(E) Competent authorities and supervision

Member States must designate as the competent authorities responsible for the authorisation and prudential supervision of payment institutions either public authorities, or bodies recognised by national law or by public authorities expressly empowered for that purpose by national law, including national central banks.

- Member States must ensure that the controls exercised by the competent authorities for checking continued compliance with the prudential requirements of the Payment Services Directive are proportionate, adequate and responsive to the risks to which payment institutions are exposed. In order to check compliance, the competent authorities shall be entitled to take the following steps, in particular:

- to require the payment institution to provide any information needed to monitor compliance;

- to carry out on-site inspections at the payment institution, at any agent or branch providing payment services under the responsibility of the payment institution, or at any entity to which activities are outsourced;

- to issue recommendations, guidelines and, if applicable, binding administrative provisions; and
- to suspend or withdraw authorisation in cases referred to in article 12 of the Payment Services Directive.

Without prejudice to the procedures for the withdrawal of authorisations and the provisions of criminal law, the Member States shall provide that their respective competent authorities, may, as against payment institutions or those who effectively control the business of payment institutions which breach laws, regulations or administrative provisions concerning the supervision or pursuit of their payment service business, adopt or impose in respect of them penalties or measures aimed specifically at ending observed breaches or the causes of such breaches.

(iv) Private law aspects of the Payment Services Directive

The private law aspects of the Payment Services Directive concern the relationship between the payment service provider and the payment service user. These provisions are, as a general rule, beneficial for the payment service user.

(A) Transparency of conditions and information requirements for payment services

Title III of the Payment Services Directive lays down rules on transparency of conditions and information requirements for payment services. This Title applies to single payment transactions, framework contracts and payment transactions covered by them.

A general distinction is being made between information obligations for single payment transactions not covered by a framework contract and information obligations for payment transactions covered by a framework contract.

As far as single payment transactions not covered by a framework agreement are concerned, a distinction is being made between i) general information requirements, ii) information for the payer after receipt of the payment order and iii) information for the payee after execution of the payment transaction.

As far as payment transactions covered by a framework agreement are concerned, the following information must be provided to the payment service user: i) general information on the payment service provider, ii) information on the use of the payment service, iii) information on charges, interests and exchange rates, iv) information on communication, v) information on safeguards and corrective measures, vi) on changes in and termination of the framework contract, and vii) information on redress.

(B) Rights and obligations in relation to the provision and use of payment services

Title IV of the Payment Services Directive lays down all rights and obligations of both the payment service provider as the payment service user in relation to the provision and use of payment services.

These rights and obligations are categorized under the following chapters:

- authorization of payment transactions. E.g., the payment service provider has the right to block the payment instrument for objectively justified reasons related to the security of the payment instrument, the suspicion of unauthorised or fraudulent use of the payment instrument or, in the case of a payment instrument with a credit line, a significantly increased risk that the payer may be unable to fulfil his liability to pay. This chapter also provides for a liability clause in case of unauthorized payment transactions. As a general rule, the payer shall bear the losses relating to any unauthorised payment transactions, up to a maximum of EUR 150, resulting from the use of a lost or stolen payment instrument or, if the payer has failed to keep the personalised security features safe, from the misappropriation of a payment instrument (this limit would not apply in cases of fraud, or where the payer has "with intent or gross negligence" failed to notify the payment service provier of losing of a card, or failing to take reasonable security steps);

- execution of payment transactions. This chapter lays down provisions on payment orders, execution time and value date and liability;
- data protection; and
- out-of-court complaint and redress procedures for the settlement of disputes.

(b) Payment Services Directive II

(i) Introduction

In July 2013, the European Commission adopted a proposal for a directive of the European Parliament and of the Council *on payment services in the internal market and amending Directives 2002/65/EC, 2013/36/EU and 2009/110/EC and repealing Directive 2007/64/EC* (hereinafter ***PSD II***).

The proposal has not yet been adopted by the European legislator, being the European Parliament and the Council of the European Union.

(ii) Proposed changes vis-à-vis the Payment Services Directive

The following short summary sketches the main proposed modifications compared to current Payment Services Directive:

(A) Changes in scope

The Payment Services Directive's provisions on transparency and information requirements will also apply in relation to payment transactions to third countries, when only one of the payment service providers is located within the European Union (so called 'one-leg transactions'), as regards those parts of the payments transaction which are carried out in the European Union.

The Payment Services Directive's provisions on transparency and information requirements will be extended to apply to all currencies and not, as currently, only to EU currencies.

The 'commercial agent' exemption has been amended to only apply to commercial agents which act on behalf of either the payer or the payee, and not to those which act for both payer and the payee. The exemption under the current Payment Services Directive has increasingly been used with regard to payment transactions handled by e-commerce platforms on behalf of both the seller (payee) and the buyer (payer). This use goes beyond the purpose of the exemption and should thus be further circumscribed.

The 'limited network' exemption has increasingly been applied to large networks involving high payment volumes and ranges of products and services. This clearly goes beyond the original purpose of this exemption, leaving large volumes of payments outside the regulatory framework and creating a competitive disadvantage for regulated market actors. The new definition, which is in line with the definition of limited networks set out in the e-money Directive, should contribute to reducing these risks.

The current digital content or 'telecom' exemption is redefined with a more restricted focus as it will apply exclusively to ancillary payment services carried out by providers of electronic communication networks or services, as for example telecom operators. The exemption will apply for the provision of digital content furnished by a third party, subject to certain thresholds set out in this directive. The new definition should ensure a level playing field between different providers and address in a more efficient way the consumer protection needs in the context of payments.

The exemption of ATM services offered by independent ATM deployers from the Payment Services Directive led to the creation of ATM networks where consumers were charged high fees for ATM withdrawals. It appears that this provision has provided incentives to the existing bank-owned ATM networks to cancel their current contractual relation with other payment service providers in order to be able to charge higher fees directly on consumers. This exemption has been deleted in the proposal for a PSD II.

(B) Safeguarding requirements

These requirements will be streamlined and the safeguarding requirements for payment institutions licensed under the PSD will be harmonised further, in particular reducing current possibilities for Member States to limit safeguarding requirements and reduce the number of possible safeguarding methods with a view to an enhanced level playing field and improved legal certainty.

(C) Web portal with EBA

A unique electronic access point within EBA should provide for enhanced transparency of authorised and registered payment institutions by providing for the interconnection at Union level of national public registers.

(D) Waiver conditions

The possibility to use a ‘lighter regime’ for ‘small payment institutions’ will be expanded to cover a higher number of small institutions, given that some Member States have had negative experiences (such as insolvency) with small payment service providers with activities beyond the current threshold for the waiver regime. The purpose is to achieve the right balance while, on the one hand, avoid unnecessary regulatory burden for very small institutions and, on the other hand, making sure that payment services’ users enjoy an adequate level of protection.

(E) Access to payment systems

PSD II fine-tunes the rules around access to payment systems by clarifying the conditions of non-direct access of payment institutions to payment systems designated under Directive 98/26/EC (Settlement Finality Directive) in a way comparable to the access used by smaller credit institutions.

(F) Surcharging

PSD II will harmonise surcharging practices further, taking due account of Directive 2011/83 on consumer rights and of the Commission proposal for a Regulation (EU) of the European Parliament and of the Council *on interchange fees for card-based payment transactions*, which was presented in parallel with PSD II. The flexibility under the current Payment Services Directive, allowing merchants to request from the payer a charge, offer him a reduction or otherwise steer him towards the use of the most efficient payment means, with the qualifier that Member States may forbid or limit any such surcharging for its territory, has led to heterogeneity in the market. Thirteen Member States have used this option to prohibit surcharges under the current PSD. The different regimes in place in Member States create problems and confusion for merchants and consumers alike, notably when selling or purchasing goods and services cross-border via the internet. The proposed prohibition of surcharging is directly linked to the capping of interchange fees according to the abovementioned proposal for a Regulation on interchange fees for card-based transactions. Given the significant reduction of the fees that the merchant will have to pay to his bank, surcharging is no longer justified for the MIF-regulated cards which will represent more than 95% of the consumer card market. The proposed rules will thus contribute to a better consumer experience when paying with a card throughout the Union and to a greater usage of payment cards instead of use of cash. As regards cards not subject to the Regulation of interchange fees as per the abovementioned proposal on interchange fees for card-based transactions, i.e. corporate cards and three-party scheme cards, merchants will still be allowed to surcharge, as long as the surcharge corresponds to the real cost incurred, taking due account of Directive 2011/83.

(G) Liability for unauthorized transactions and refunds

The proposed modifications will streamline and further harmonise the liability rules in case of unauthorised transactions, ensuring enhanced protection of the legitimate interests of payment users. Except in case of fraud and gross negligence, the maximum amount a payment user could under any circumstances be obliged to pay in case of an unauthorised payment transaction will be decreased from the current amount of 150 EUR to 50 EUR. It will also clarify that late payments do not necessarily trigger a refund.

PSD II introduces new rules on refunds for payment transactions initiated by or through a payee. This clarifies the refund right for direct debit transactions bringing it in line with the SEPA Core Direct Debit Rulebook, provided that the good or service paid for has not yet been consumed. Under the current rules, different refund regimes apply regarding direct debits, depending on whether a prior authorisation has been given, the amount exceeds the amount expected or whether, alternatively, a further right had been agreed.

(H) Security measures

The proposed rules address security aspects and aspects of authentication in line with the Commission proposal for a Directive of the European Parliament and Council *on network and information security*.

(I) Coverage of new services

Title I-V and Annex I point 7: coverage of new services and service providers enabling access to payment accounts. The current PSD does not cover these actors insofar as they do not dispose of the payer's or payee's fund at any time. The fact that these third party service providers are currently unregulated, at least in certain Member States, has raised security, data protection and liability concerns, despite the potential benefits brought by these services and service providers. The proposal brings third party service providers offering notably online banking based payment initiation services under the scope of the Payment Services Directive (Annex I point 7). This should enhance new low cost e-payment solutions on the internet while ensuring appropriate security, data protection and liability standards. In order to be allowed to provide payment initiation services, third party service providers would be required to get licensed or registered and supervised as payment institutions (Title II. Like other payment service providers, they will be subject to harmonised rights and obligations, and in particular security requirements (articles 85 and 86). The envisaged rules will in particular address conditions for access to account information (article 58), requirements regarding authentication (article 87) and rectification of transactions (articles 63 and 64) and a balanced liability repartition (articles 65 and 66). New payment services providers will benefit from this new regime, regardless of whether they dispose of the payer's or payee's funds at any time.

(J) Out-of-court complaint and redress procedures and sanctions

Chapter 6 - Out-of-Court complaint and redress procedures for the settlement of disputes - shall enhance effective compliance with the Directive. The new measures update the requirements on out of court complaint and redress procedures and appropriate penalties.

Member States will be obliged to align administrative sanctions, ensure that appropriate administrative measures and sanctions are available for breaches of the Directive and ensure that these sanctions are duly applied.

(K) European Banking Authority

The Directive contains several areas where work by EBA in its capacity of contributing to the consistent and coherent functioning of supervision is foreseen (as referred to in Regulation (EU) 1093/2010). In particular, EBA will be asked to issue guidelines and draft regulatory technical standards in various fields, for example in order to clarify the rules on 'passporting' for payment institutions operating in several Member States, or to ensure the establishment of adequate security requirements.

(iii) Status of the legislative process of PSD II

The European Commission's proposal for PSD II has not yet been finally adopted by the European legislator (being the Council of the European Union and the European Parliament). The European Parliament already made substantial amendments to the proposal. After adoption of the directive, Member States will have to transpose the directive into national law within a certain timeframe (usually two years after adoption of the directive).

(c) E-money Directive

(i) Introduction

The e-money Directive has been adopted on 16 September 2009, and Member States were required to implement the Directive by 30 April 2011.

The e-money Directive lays down rules on the taking up, pursuit and prudential supervision of the business of electronic money institutions.

(ii) Scope

For the scope of the e-money Directive we refer to section 1.2 of this memorandum.

(iii) Public law aspects

(A) Licensing requirements

Articles 5 and 10 to 15, article 17(7) and articles 18 to 25 of the Payment Services Directive apply to electronic money institutions *mutatis mutandis*.

This implies that all rules of the Payment Services Directive in relation to the application for authorisation, granting of authorisation, withdrawal of authorization, communication of the decision to grant the authorization, maintenance of authorization, registration, outsourcing and the rules on competent authorities and supervision will apply *mutatis mutandis* to e-money institutions. For a description of these rules, we refer to the relevant sections on the Payment Services Directive above.

(B) Capital requirements

Member States shall require electronic money institutions to hold, at the time of authorisation, initial capital of not less than EUR 350 000.

(C) Activities

In addition to issuing electronic money, electronic money institutions shall be entitled to engage in any of the following activities:

- the provision of payment services listed in the Annex to the Payment Services Directive;
- the granting of credit related to payment services referred to in points 4, 5 or 7 of the Annex to the Payment Services Directive, where the conditions laid down in article 16(3) and (5) of that Directive are met;

- the provision of operational services and closely related ancillary services in respect of the issuing of electronic money or to the provision of payment services referred to in point (a);
- the operation of payment systems as defined in point 6 of article 4 of the Payment Services Directive and without prejudice to article 28 of that Directive;
- business activities other than issuance of electronic money, having regard to the applicable EU and national law.

Credit referred to in point (b) of the first subparagraph shall not be granted from the funds received in exchange of electronic money and held in accordance with article 7(1) of the e-money Directive.

Electronic money institutions shall not take deposits or other repayable funds from the public.

(iv) Issuance and redeemability of electronic money

The e-money Directive lays down certain provisions on the issuance and redeemability of electronic money.

Member States shall ensure that electronic money issuers issue electronic money at par value on the receipt of funds. Member States shall ensure that, upon request by the electronic money holder, electronic money issuers redeem, at any moment and at par value, the monetary value of the electronic money held.

Member States shall prohibit the granting of interest or any other benefit related to the length of time during which an electronic money holder holds the electronic money.

(d) SEPA Regulation

(i) Introduction

Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012 *establishing technical and business requirements for credit transfers and direct debits in euro and amending Regulation (EC) No 924/2009* (hereinafter ***the SEPA Regulation***) lays down rules on credit transfers and direct debits in euro and constitutes an essential legislative piece in the legal framework of SEPA.

The SEPA Regulation entered into force in March 2012 and is directly applicable in all Member States of the EU, without transposition into national law being necessary.

(ii) Scope

The SEPA Regulation lays down rules for credit transfer and direct debit transactions denominated in euro within the Union where both the payer's payment service provider and the payee's payment service provider are located in the Union, or where the sole payment service provider involved in the payment transaction is located in the Union.

- The SEPA Regulation does not apply to the following:
- payment transactions carried out between and within payment service providers, including their agents or branches, for their own account;
- payment transactions processed and settled through large-value payment systems, excluding direct debit payment transactions which the payer has not explicitly requested be routed via a large-value payment system;
- payment transactions through a payment card or similar device, including cash withdrawals, unless the payment card or similar device is used only to generate the information required

to directly make a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN;

- payment transactions by means of any telecommunication, digital or IT device, if such payment transactions do not result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN;
- transactions of money remittance as defined in point (13) of article 4 of the Payment Services Directive;
- payment transactions transferring electronic money as defined in point (2) of article 2 of the e-money Directive, unless such transactions result in a credit transfer or direct debit to and from a payment account identified by BBAN or IBAN.
- Key features of the SEPA Regulation
- The key provisions of the SEPA Regulation are listed below:
- Article 3 lays down the principle of reachability. This implies that when payment service providers offer domestic credit transfer and direct debit services, they must be able to execute the same type of services or transactions on a cross-border basis as well.
- Article 4 lays down the principle of interoperability. This means that payment schemes of payment service providers need to comply with a number of conditions: credit transfers and direct debits may not be hampered by technical restrictions, the rules related to payment schemes need to be the same for domestic and cross-border credit transfers and direct debits, and so on. This principle is introduced in order to improve competition in the market. It is essential for the creation of a unified payment area, that credit transfers and direct debits are not hampered by local, domestic sector prescriptions or technical restrictions.
- Article 5 lays down a highly-detailed number of technical requirements for credit transfers and direct debits. This article introduces the SEPA Credit Transfer (hereinafter ***SCT***) and the SEPA Direct Debit (hereinafter ***SDD***), which constitute the cornerstone of the SEPA Regulation. This article provides for a number of technicalities with which the SCT and the SDD will need to comply: mandatory use of BIC and IBAN, mandatory use of the ISO20022 format, and the specification of a number of essential data such as the amount of the transaction.
- Article 7 concerns the situation of direct debits initiated before 1 February 2014 and which are still operational today. In sum, this provisions provides that such direct debits are still valid today.
- Article 8 relates to multilateral interchange fees for direct debits. One of the main goals of the European legislator with regard to this provision is the creation of a level playing field between payment service providers. For this reason, the SEPA regulation provides that no multilateral interchange fees may be charged for direct debits. There is one exemption for R-transactions: these are transactions which have been reversed, rejected, returned or refused (due to a lack of credit, a wrong amount or date, wrong account number, and so on). Multilateral interchange fees can still be applied to such R-transactions, but under certain conditions (cost-based, not higher than real incurred costs and only in order to attribute it to the payment service provider who caused the R transaction).

(iii) Migration deadline

The official migration deadline to be compliant with the SEPA Regulation was set at 1 February 2014.

Because of the statistical evidence highlighting the substantial number of market participants not having migrated and the potential for disruption, the European legislator adopted a regulation early 2014 to allow for a 6-month transitional period until 1 August 2014.

According to the quantitative SEPA indicators published by the ECB, the share of SEPA Credit Transfer transactions amounted to 99.4 percent in August 2014. Furthermore, the share of SEPA Direct Debit transactions had reached 99.9 percent. The quantitative SEPA indicators measure the share of SCT and SDD transactions as a percentage of the total volume of credit transfers and direct debits generated by bank customers in the euro area. The SEPA migration is therefore deemed completed.

(e) Regulation on cross-border payments

Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009 *on cross-border payments in the Community and repealing Regulation (EC) No 2560/2001* (hereinafter ***the Regulation on cross-border payments***) eliminates the differences in charges for cross-border and national payments in euro. It applies to payments in euro in all EU Member States. The basic principle is that the charges for payment transactions offered by a payment service provider (e.g. a credit institution) have to be the same, for the payment of the same value, whether the payment is national or cross-border.

The Regulation on cross-border payments applies to all electronically processed payments, including credit transfers, direct debits, cash withdrawals at cash dispensers (ATMs), payments by means of debit and credit cards, and money remittance. Some conditions may apply depending on the type of a payment transaction. For example, for credit transfers and direct debits, the use of IBAN and BIC when ordering the payment, is obligatory.

All non-euro area Member States have the possibility to extend the application of the Regulation on cross-border payments and to apply the same charges for payments in euro as for payments in their national currency.

(f) The European Payments Council: SEPA rulebooks

The European Payments Council (hereinafter ***EPC***) supports and promotes the creation of SEPA.

The EPC is the decision-making and coordination body of the European banking industry in relation to payments. The EPC develops the payment schemes and frameworks which help to realise SEPA. Note that the EPC is not part of the institutional framework of the European Union.

EPC members represent banks, banking communities and payment institutions. More than 360 professionals are directly engaged in the EPC's work programme, representing organisations of all sizes and sectors of the European banking industry. The ECB acts as an observer in all EPC working and support groups and in the EPC Plenary (the Plenary is the decision-making body of the EPC). The EPC is an international not-for-profit association which makes all of its deliverables, including the SEPA Scheme Rulebooks and adjacent documentation, available to download free of charge on the EPC Website. The EPC does not supply technology, goods or services.

The EPC develops, among other things, the SEPA payment schemes as defined in the SEPA Credit Transfer (SCT) and SEPA Direct Debit (SDD) Rulebooks. The rulebooks contain sets of rules and standards for the execution of SEPA payment transactions that have to be followed by adhering payment service providers. These rulebooks can be regarded as instruction manuals which provide a common understanding on how to move funds from account A to account B within SEPA. The schemes are based on technical standards defined by standards bodies such as the International Organization for Standardization. The SEPA payment schemes developed by the EPC have open access criteria in line with article 28 of the Payment Services Directive.

A detailed description of these SEPA rulebooks falls outside the scope of this memorandum.

(g) Financial Conglomerates Directive

(i) Introduction

We understood that you wish us to elaborate on the Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 *on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate* (hereinafter ***the Financial Conglomerates Directive***), as amended by Directive 2011/89/EU of the European Parliament and of the Council of 16 November 2011 *amending Directives 98/78/EC, 2002/87/EC, 2006/48/EC and 2009/138/EC as regards the supplementary supervision of financial entities in a financial conglomerate*.

(ii) Scope

The Financial Conglomerates Directive lays down rules for supplementary supervision of regulated entities which have obtained an authorisation pursuant to the respective directives that apply to them, and which are part of a financial conglomerate.

Regulated entity means a credit institution, an insurance undertaking, a reinsurance undertaking, an investment firm, an asset management company or an alternative investment fund manager. Payment institutions or e-money institutions are not listed as regulated entities (but may form part of a financial conglomerate).

- A financial conglomerate means a group which meets the following conditions:
- a regulated entity is at the head of the group or at least one of the subsidiaries in the group is a regulated entity;
- where there is a regulated entity at the head of the group, it is either a parent undertaking of an entity in the financial sector, an entity which holds a participation in an entity in the financial sector, or an entity linked with an entity in the financial sector by a relationship within the meaning of article 12(1) of Directive 83/349/EEC;
- where there is no regulated entity at the head of the group, the group's activities mainly occur in the financial sector within the meaning of article 3(1);
- at least one of the entities in the group is within the insurance sector and at least one is within the banking or investment services sector;
- the consolidated and/or aggregated activities of the entities in the group within the insurance sector and the consolidated and/or aggregated activities of the entities within the banking and investment services sector are both significant within the meaning of article 3(2) or (3).

(iii) Supplementary supervision

Supplementary supervision focuses on problems that can arise from:

- Multiple use of capital: supervisors are to make sure that capital is not used twice or more within a conglomerate. For example, funds may not be included in the calculation of capital on both the level of the single entity and the parent entity.
- Group risks: Group risks are risks that arise from the group structure and which are not related to specific banking or specific insurance business. They refer to risks of contagion (when risks spread from one end of the group to another), management complexity (managing more than 1.000 legal entities is a far more difficult challenge than managing 20 legal entities), risk concentration (the same risk materialising in several parts of the group at the same time), and conflicts of interest (e.g. one part of the group has an interest in selling an exposure, while another part of the group has an interest in keeping that exposure).

The Financial Conglomerates Directive allows national supervisors to monitor those risks, for example by requiring conglomerates to provide additional reporting. Supervisors can also require conglomerates to present additional risk management or internal governance measures. The Financial Conglomerates Directive also requires supervisors to cooperate across sectors and across borders in order to control possible group risks.

(h) Anti-money laundering obligations for payment service providers and issuers of e-money

(i) Regulation 1781/2006 on information on the payer accompanying transfers of funds

Regulation (EC) No 1781/2006 of the European Parliament and of the Council of 15 November 2006 *on information on the payer accompanying transfers of funds* (hereinafter ***the Funds Transfer Regulation***) lays down rules on information on the payer to accompany transfers of funds for the purposes of the prevention, investigation and detection of money laundering and terrorist financing.

The regulation transposes Special Recommendation VII (SRVII) of the Financial Action Task Force (FATF) into EU law and is part of the EU Plan of Action to Combat Terrorism.

This regulation applies to transfers of funds, in any currency, which are sent or received by a payment service provider established in the European Union (with certain exemptions such as certain transfers of funds carried out by means of a mobile telephone).

The regulation lays down certain information requirements to the payment service provider of both the payer and the payee, in order to make sure that both the payer and the payee are sufficiently identified.

A detailed description of these information requirements falls outside the scope of this memorandum. We can further elaborate in more detail upon request.

(ii) Third EU Anti-Money Laundering Directive

(A) Introduction

On an EU level, money laundering is regulated by Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 *on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (hereinafter ***the 3rd EU Anti-Money Laundering Directive***).

This directive sets out to prevent the financial system from being used for money laundering and terrorist financing, and repeals Directive 91/308/EEC.

European Union (EU) countries must prohibit money laundering and the financing of terrorism. To this end, they may adopt or retain in force stricter provisions than provided for in this directive.

Payment Institutions’ and e-money institutions' compliance with anti-money laundering and counter terrorist financing obligations is a prerequisite for their authorisation under the Payment Services Directive (article 5 of the Payment Services Directive).

(B) Key obligations under the EU Anti-Money Laundering Directive

The entities and persons covered by the Anti-Money Laundering Directive are required to apply customer due diligence measures when establishing a business relationship or when carrying out occasional transactions amounting to EUR 15 000 or more. Furthermore, they must file a suspicious transaction report when there is suspicion of money laundering or terrorist financing, regardless of any exemption or threshold.

These diligence measures involve identifying the customer and verifying his/her identity, obtaining information on the purpose and intended nature of the business relationship and, where appropriate, identifying and verifying the identity of the natural person owning or controlling the customer or on whose behalf the activity is carried out. The extent of such measures may be determined on a risk-based approach depending, for example, on the type of customer or business relationship. EU countries may allow the entities and persons covered by the directive to call on third parties to execute the customer due diligence measures. The directive also lists cases in which simplified customer due diligence measures may be used, such as in relation to national public authorities, customers with life insurance policies with an annual premium of no more than EUR 1 000 or electronic money holders.

Where there is a high risk of money laundering or terrorist financing, the entities and persons covered by the directive are required to apply enhanced customer due diligence. Enhanced customer due diligence involves supplementary measures to verify or certify the documents supplied when the customer has not been physically present for identification purposes.

Finally, credit and other financial institutions may not keep anonymous accounts or anonymous passbooks.

European countries are required to inform each other and the European Supervisory Authorities (ESA), namely the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA) and the European Securities and Markets Authority (ESMA) where they believe that a third country meets the equivalence conditions concerning the assessment of situations which represent a low risk of money laundering and terrorist financing.

Each EU country must set up a financial intelligence unit (FIU) in the form of a central national unit. These units are responsible for receiving, requesting, analysing and disseminating to the competent authorities information concerning potential money laundering or terrorist financing. EU countries must provide their FIU with adequate resources to fulfil its tasks and ensure that it has access to any necessary financial, administrative and law enforcement information.

The entities and persons covered by the directive must file a suspicious transaction report without delay to the FIU when they know or suspect that money laundering or terrorist financing is being or has been committed or attempted. In the meantime, they must refrain from carrying out transactions. At the FIU's request, these entities and persons must furnish all necessary information in accordance with the applicable legislation.

EU countries may decide whether they require independent legal professions, notaries, auditors, external accountants and tax advisers to inform the FIU of information they receive from or obtain on their clients when ascertaining the legal position of their client or when defending or representing that client in judicial proceedings.

The entities and persons covered by the directive may not reveal to the customer or to other third persons that information has been transmitted to the FIU, except in the case of law enforcement. They must keep documents and supporting or other evidence for at least five years from the end of the business relationship or the carrying-out of the transaction.

Member States are required to inform each other and the EAS where they believe that a third country meets the equivalence conditions concerning the prohibition of disclosure, professional secrecy and personal data protection.

The entities and persons covered by the directive must establish appropriate measures and procedures for customer due diligence, reporting of information, record keeping, risk management and communication. They must ensure that the relevant employees are aware of the provisions in force.

EU countries must monitor compliance with the directive. The entities and persons concerned must be held liable for any failure to comply with the national provisions adopted pursuant to the directive. The penalties must be effective, proportionate and dissuasive.

(C) Specific derogation for e-money

By way of derogation from articles 7(a), (b) and (d), 8 and 9(1) of the Anti-Money Laundering Directive, Member States may allow the institutions and persons covered by the Anti-Money Laundering Directive not to apply customer due diligence in respect of electronic money, as defined in the e-money Directive, where, if the device cannot be recharged, the maximum amount stored in the device is no more than EUR 150, or where, if the device can be recharged, a limit of EUR 2 500 is imposed on the total amount transacted in a calendar year, except when an amount of EUR 1 000 or more is redeemed in that same calendar year by the bearer.

5. Future changes in the EU legislative framework on payment services

5.1 Article 87 of the Payment Services Directive: status

(a) Article 87 of the Payment Services Directive

Article 87 of the Payment Services Directive stipulates that by 1 November 2012, the European Commission had to present to the European Parliament, the Council, the European Economic and Social Committee and the European Central Bank a report on the implementation and impact of the Payment Services Directive, in particular on:

- the possible need to extend the scope of the Payment Services Directive to payment transactions in all currencies and to payment transactions where only one of the payment service providers is located in the European Union,
- the application of articles 6, 8 and 9 concerning prudential requirements for payment institutions, in particular as regards own funds requirements and safeguarding requirements (ringfencing),
- the possible impact of the granting of credit by payment institutions related to payments services, as set out in article 16(3),
- the possible impact of the authorisation requirements of payment institutions on competition between payment institutions and other payment service providers as well as on barriers to market entry by new payment service providers,
- the application of articles 34 and 53 and the possible need to revise the scope of the Directive with respect to low value payment instruments and electronic money, and
- the application and functioning of articles 69 and 75 for all kinds of payment instruments,

accompanied, where appropriate, by a proposal for its revision.

(b) Report from the European Commission on the application of the Payment Services Directive

The report referred to in article 87 of the Payment Services Directive was finalized on 24 July 2013.

In this report the European Commission identified a number of issues with regard to the Payment Services Directive. These issues relate to, among others, the scope of the directive, one-leg transactions and transactions in all currencies, authorisation requirements and barriers to market entry, prudential requirements, granting of credit by payment institutions, execution time and non-execution or defective execution.

The report further describes the transposition of the Payment Services Directive in the different Member States, considers its application and impacts, identifies main issues emerging from the application of the Payment Services Directive and draws a number of conclusions.

(c) PSD II: legislative status

This report eventually led to a proposal of the European Commission for PSD II.

For an overview of all key changes of PSD II vis-à-vis the Payment Services Directive, we refer to section 2.2 (b) of this memorandum.

Currently, PSD II has not yet been adopted by the European legislator. At the European Parliament Plenary session held on 3 April 2014, the European Parliament voted to adopt amendments to the proposal. Discussions on the proposal and the changes put forward by the European Parliament have now moved to the Council of the European Union.

As a directive, the provisions of PSD II will need to be transposed into national law by Member States, typically within two years after its adoption.

5.2 Future changes to the EU payment services framework

(a) Proposal for a PSD II

Please refer to the sections above for a review of the legislative developments regarding PSD II.

(b) Proposal for an EU Regulation on Multilateral Interchange Fees

On 24 July 2014, the European Commission published a proposal for a regulation of the European Parliament and of the Council *on interchange fees for card-based payment transactions* (hereinafter ***MIF Regulation***).

The MIF Regulation mainly deals with the issue of so-called "Multilateral Interchange Fees" (MIFs).

According to the European Commission, one of the key practices hindering the achievement of an integrated market is the widespread use in 'four party' schemes, the most common type of card schemes, of Multilateral Interchange Fees.

MIFs are collectively agreed inter-bank fees usually between the acquiring payment service providers and the issuing payment service providers belonging to a certain scheme. Such interchange fees paid by acquiring payment service providers form part of the fees they charge to merchants (the Merchant Service Charges or MSCs), which merchants in turn pass on to consumers. Thus, high Interchange Fees paid by merchants result in higher final prices for goods and services, which are paid by all consumers.

Essentially, the European Commission proposes to cap the Multilateral Interchange Fees.

After a transitional period (during which only cross-border transactions are envisaged), all cross-border and domestic 'consumer' debit card transactions and card-based payment transactions based on such a transaction will have a maximum interchange fee of 0,20% and all cross-border and domestic consumer credit card transactions and card based payment transactions based on those will have a maximum interchange fee of 0.30%.

Other elements of the MIF Regulation relate to:

- the prohibition of circumvention fees: for the purpose of implementing the MIF caps, the net compensation of fees received and paid between the issuer and the scheme are integrated in the calculation of the interchange fees paid and received for the purpose of assessing possible circumvention;

- licensing: the licenses delivered by schemes for issuing or acquiring purposes are not restricted to a specific territory but cover the entire Union territory;
- separation between scheme and processing: an organisational separation should be in place between the schemes and the entities which are processing the transactions;
- co- badging and choice of application: the issuer of the payment instrument decides whether the payment application can reside on the same card or wallet. The choice of payment application used remains with the consumer and cannot not be prescribed in advance by the issuer through automatic mechanisms on the instrument or the equipment at the point of sale;
- unblending: acquiring banks shall offer and charge payees individually for different categories and different brands of payment cards and not impose a single price, and provide the relevant information on the amounts applicable for the different categories and brands;
- honour all cards rule: payment schemes and payment service providers cannot impose that a retailer accepts a category or brand if he accepts another category or brand, except if the brand or category is subject to the same regulated interchange fee as the former. For example, merchants accepting consumer debit cards may not be forced to accept consumer credit cards but can be imposed to accept other consumer debit cards;
- steering rules: payment schemes and payment service providers schemes cannot prevent retailers from steering consumers towards the use of specific payment instruments preferred by the retailer. This is without prejudice to the rules on rebates and surcharges established under the Payment Services Directive and article 19 of the Consumer Rights Directive. Payment schemes and payment service providers schemes cannot prevent retailers from informing consumers about interchange fees and merchant service charges;
- information for the payee on individual payment transactions: the payment service provider must provide certain information to the merchant after the execution of an individual payment transaction;
- penalties: Member States must establish rules on sanctions for breaches of the provisions in the Regulation, and must notify the European Commission of these;
- Out-of-court complaint and redress procedures: Member States must establish specific requirements for the settlement of disputes between payees and payment service providers;

The proposal has not yet been adopted by the European legislator. The proposal has already been amended by the European Parliament, and there is still a lot of discussion and lobbying ongoing.

(c) Proposal for an EU Regulation on information accompanying transfers of funds

On 5 February 2013, the European Commission published a proposal for a regulation of the European Parliament and of the Council *on information accompanying transfers of funds*.

The purpose of this proposal is to revise the Funds Transfers Regulation in ways which improve traceability of payments and ensure that the EU framework remains fully compliant with international standards.

In line with new FATF Recommendation 16 on "wire transfers" and the accompanying Interpretative note, the proposed changes are aimed at addressing areas where gaps in transparency still remain.

The intention is to enhance traceability by imposing the following main requirements:

- include information on the payee;

- with regard to the scope of the Regulation, clarify that credit or debit cards, or mobile telephone or any other digital or IT device become subject to the provisions of the regulation if they are used to transfer funds person to person. In addition, clarify that below EUR 1000, in the case of fund transfers outside the EU, a lighter regime of non-verified information on the payer and the payee applies (as opposed to possible exemptions from scope as in the Funds Transfers Regulation);

- with regard to obligations of the payment service provider of the payee, imposing a requirement to verify the identity of the beneficiary (where not previously identified) for payments originating outside the EU and where the amount is more than EUR 1000. With regard to the payment service provider of the payee and the intermediary payment service provider, an obligation to establish risk-based procedures for determining when to execute, reject or suspend a transfer of funds which lacks the required information and to determine appropriate follow-up action;

- with regard to data protection, align the requirements of record keeping of the information with the FATF standards, in accordance with the new regime foreseen by the European Commission's proposal for a new Data Protection Directive (not yet adopted);

- with regard to sanctions, reinforcement of sanctioning powers for competent authorities and a requirement to coordinate actions when dealing with cross-border cases; a requirement for sanctions imposed for breaches to be published; and a requirement to establish effective mechanisms to encourage reporting of breaches of the provisions of the Regulation.

The proposal for an EU Regulation on information accompanying transfers of funds has not yet been adopted by the EU legislator.

(d) Proposal for a 4th EU Anti-Money Laundering Directive

On 5 February 2013, the European Commission published a proposal for a Directive of the European Parliament and of the Council *on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing* (hereinafter ***the 4th Anti-Money Laundering Directive***).

The 4th Anti-Money Laundering Directive intends to revise and strengthen the 3rd Anti-Money Laundering Directive.

The main modifications to the Third Anti-Money Laundering Directive are:

- Extension of the scope of the Directive: (a) the threshold for traders in high value goods dealing with cash payments will be reduced from EUR 15000 to EUR 7500 (b) inclusion of casino's in the scope of the Directive;

- Risk-based approach:

  - Member States will be required to identify, understand and mitigate the risks facing them. This can be supplemented by risk assessment work carried out at a supra-national level (e.g. by the European Supervisory Authorities or Europol) and the results should be shared with other Member States and obliged entities;

  - Obliged entities operating within the scope of the Directive would be required to identify, understand and mitigate their risks, and to document and update the assessments of risk that they undertake;

  - The proposal would recognise that the resources of supervisors can be used to concentrate on areas where the risks of money laundering and terrorist financing are greater.

- Simplified and enhanced customer due diligence: in the proposal, obliged entities would be required to take enhanced measures where risks are greater and may be permitted to take simplified measures where risks are demonstrated to be less.

- Information on the beneficial owner: the revised Directive proposes new measures in order to provide enhanced clarity and accessibility of beneficial ownership information. It requires legal persons to hold information on their own beneficial ownership.

- Third country equivalence: the revised Directive will remove the provisions relating to positive "equivalence", as the customer due diligence regime is becoming more strongly risk-based and the use of exemptions on the grounds of purely geographical factors is less relevant.

- Administrative sanctions: the revised Directive contains a range of sanctions that Member States should ensure are available for systematic breaches of key requirements of the Directive, namely customer due diligence, record keeping, suspicious transaction reporting and internal controls.

- Financial Intelligence Units: further extension and strengthening of cooperation between FIUs.

- European Supervisory Authorities (ESA): the proposal contains several areas where work by the ESA is envisaged. In particular, EBA, EIOPA and ESMA are asked to carry out an assessment and provide an opinion on the money laundering and terrorist financing risks facing the EU.

- Data Protection: the need to strike a balance between allowing robust systems and controls and preventative measures against money laundering and terrorist financing on the one hand, and protecting the rights of data subjects on the other is reflected in the proposal.

- Transposition measures: Due to the complexity and scope of the proposal, Member States are required to transmit a correlation table of the provisions of their national law and the Directive.

6. Specific Q&A

Under EU law, do capital requirements and safeguarding requirements vary based upon the type of payment service providers (e.g. credit institutions, payment institutions, or electronic money institutions) or type of services? If so, could you tell us the reason for the variation?

6.1 Differences in capital requirements

(a) Payment institutions

Member States shall require payment institutions to hold, at the time of authorisation, initial capital, comprised of the items defined in Article 57(a) and (b) of Directive 2006/48/EC as follows:

- where the payment institution provides only the payment service listed in point 6 of the Annex, its capital shall at no time be less than EUR 20 000 (i.e. initial capital for money remitters);

- where the payment institution provides the payment service listed in point 7 of the Annex, its capital shall at no time be less than EUR 50 000 (i.e. initial capital for mobile payments); and

- where the payment institution provides any of the payment services listed in points 1 to 5 of the Annex, its capital shall at no time be less than EUR 125 000 (i.e. initial capital for full-range payment service providers).

Notwithstanding the initial capital requirements set out above, Member States must require payment institutions to hold, at all times, own funds calculated in accordance with one of the three methods (A, B or C) as defined in article 8 of the PSD. These three methods to calculate own funds, can be briefly summarized as follows:

- Method A: 10% of fixed overheads (administrative expenses, rent, salaries, etc);
- Method B: degressive percentage (from 4% to 0.25%) of the amount of monthly payment transactions in the previous year; or
- Method C: degressive percentage (from 10% to 1.5%) of the sum of the relevant indicator (sum of interest income, interest expense, commissions & fees, other operating income).

(b) Credit institutions

On an EU level, capital requirements for credit institutions are regulated by the CRR and the CRD ("the CRD IV package"). According to article 12 of the CRD the competent authorities of the Member States must refuse authorisation to commence the activity of a credit institution where a credit institution does not hold separate own funds or where its initial capital is less than EUR 5 million.

Ongoing capital requirements for credit institutions comprises a highly complex set of rules and falls outside the scope of this research paper.

(c) E-money institutions

According to article 4 of the e-money Directive, Member States must require e-money institutions to hold, at the time of authorisation, initial capital, comprised of the items set out in Article 57(a) and (b) of Directive 2006/48/EC, of not less than EUR 350 000.

E-money institutions are to hold own funds which, as stated in Directive 2006/48/EC, shall be composed mainly of capital, reserves, funds for general banking risks, revaluation reserves and value adjustments. They shall mainly be calculated according to the following methods:

- for activities not related to the issuance of e-money, own funds shall be calculated in accordance with methods A, B or C of Article 8 of the PSD;
- for the activity of issuing e-money, own funds shall amount to at least 2% of the average outstanding electronic money.

(d) Reason for the variation in capital requirements

Credit institutions hold deposits which they use for a variety of risk-taking activities, including providing credit, and can pose a systemic risk to the wider financial system. On the other hand, payments institutions cannot take deposits, cannot use funds in a payment account to finance its payment activities (including possible credit granting). Payment institutions are therefore subject to an extremely low level of risk which does not pose a systemic risk to the financial system (but even so payment institutions are still subject to oversight arrangements by the ECB and national central banks).

6.2 Differences in safeguarding requirements

(a) Payment institutions

The Member States or competent authorities must require a payment institution which provides any of the payment services listed in the Annex and, at the same time, is engaged in other business activities referred to in Article 16(1)(c) to safeguard funds which have been received from the payment service users or through another payment service provider for the execution of payment transactions, as follows:

either:

- they shall not be commingled at any time with the funds of any natural or legal person other than payment service users on whose behalf the funds are held and, where they are still held by the payment institution and not yet delivered to the payee or transferred to another payment service provider by the end of the business day following the day when the funds have been received, they shall be deposited in a separate account in a credit institution or invested in secure, liquid low-risk assets as defined by the competent authorities of the home Member State; and

- they shall be insulated in accordance with national law in the interest of the payment service users against the claims of other creditors of the payment institution, in particular in the event of insolvency; or

- they shall be covered by an insurance policy or some other comparable guarantee from an insurance company or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which would have been segregated in the absence of the insurance policy or other comparable guarantee, payable in the event that the payment institution is unable to meet its financial obligations.

Where a payment institution is required to safeguard funds and a portion of those funds is to be used for future payment transactions with the remaining amount to be used for non-payment services, that portion of the funds to be used for future payment transactions shall also be subject to the requirements above. Where that portion is variable or unknown in advance, Member States may allow payment institutions to apply this paragraph on the basis of a representative portion assumed to be used for payment services provided such a representative portion can be reasonably estimated on the basis of historical data to the satisfaction of the competent authorities.

The Member States or competent authorities may require that payment institutions which are not engaged in other business activities referred to in Article 16(1)(c) of the PSD shall also comply with the safeguarding requirements as elaborated above.

The Member States or competent authorities may also limit such safeguarding requirements to funds of those payment service users whose funds individually exceed a threshold of EUR 600.

(b) Credit institutions

A detailed analysis of credit institution's safeguarding requirements falls outside the scope of this memorandum. As a general rule, credit institutions must segregate a client's assets from its own assets (i.e. assets should be kept on different accounts in order to prevent commingling of assets).

(c) E-money institutions

Member States must require an e-money institution to safeguard funds that have been received in exchange for electronic money that has been issued, in accordance with Article 9(1) and (2) of the PSD. Funds received in the form of payment by payment instrument need not be safeguarded until they are credited to the e-money institution’s payment account or are otherwise made available to the e-money institution in accordance with the execution time requirements laid down in the PSD, where applicable. In any event, such funds shall be safeguarded by no later than five business days, as defined in point 27 of Article 4 of the PSD, after the issuance of e-money.

For the purposes of the paragraph above, secure, low-risk assets are asset items falling into one of the categories set out in Table 1 of point 14 of Annex I to Directive 2006/49/EC *of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions* for which the specific risk capital charge is no higher than 1,6 %, but excluding other qualifying items as defined in point 15 of that Annex. For the purposes of the paragraph above, secure, low-risk assets are also units in an undertaking for collective investment in transferable securities (UCITS) which invests solely in the assets as specified above.

In exceptional circumstances and with adequate justification, the competent authorities of the Member States may, based on an evaluation of security, maturity, value or other risk element of the assets as specified above, determine which of those assets do not constitute secure, low-risk assets for the purposes of the first paragraph above.

Article 9 of the PSD shall apply to e-money institutions for the activities referred to in Article 6(1)(a) of the e-money Directive that are not linked to the activity of issuing e-money.

Member States or their competent authorities may determine, in accordance with national legislation, which method shall be used by the e-money institutions to safeguard funds.

- ***Are only credit institutions permitted to engage in deposit-taking activities?***

Yes.

- ***What is the difference between "deposits" and "payment account"? What business is considered as deposit-taking business?***

A "Payment account" means an account held in the name of one or more payment service users which is used for the execution of payment transactions (article 4 (14) of the PSD). Payment institutions cannot accepts deposits. Specific safeguarding requirements apply for funds received from payment service users (please refer to the sections above on safeguarding requirements).

Deposits are repayable funds received from the public (money, coins, bills, etc.) (the term "deposit" is not defined as such in CRD IV).

Only authorized credit institutions are allowed to take deposits or other repayable funds from the public. Specific safeguarding requirements apply for deposits (please refer to the sections above on safeguarding requirements).

- ***Does Article 3(b) of the PSD include payment transactions between the payer and the payee through a commercial agent authorised only to receive payment of the costs of goods or services on behalf of the payee? Would your answer be different depending on whether or not the payee's right to claim against the payer will be extinguished upon the agent's receipt of the payment?***

Article 3(b) of the PSD stipulates that the PSD shall not apply to payment transactions from the payer to the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee.

This is the so-called "commercial agent exemption". If the intermediary you are referring to in your question qualifies as a commercial agent, i.e. someone who is authorized to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee, the exemption would apply and the situation would fall outside the scope of the directive.

- ***Do the Member States or competent authorities provide the exemption, according to Article 9.4 or Article 26.1 of the PSD?***

  - Article 9 (4) of the PSD

Article 9 (4) of the PSD stipulates that the Member States or competent authorities may limit the safeguarding requirements of Payment Institutions to funds of those payment service users whose funds individually exceed a threshold of EUR 600.

This is optional. Member States may choose to implement this provision of the PSD into national law or not. E.g., Belgium did not implement this provision into national law. We are not aware whether other Member States did or did not implement this provision in their national legal framework.

- Article 26 (1) of the PSD

Article 26 of the PSD provides that Member State competent authorities may waive certain requirements and enter a payment institution onto the register. However, Article 26(1) of the PSD does set out certain requirements on the applicant and these are:

- in the preceding 12 months the applicant has operated below an average of total payment transactions per month of EUR 3 000 000;
- no individual involved in the applicant's management or operation has any previous money laundering or other financial crime convictions;
- the applicant has no desire to operate cross border and make use of the PSD passport right; and
- the applicant has its head office or, in the case of an individual, place of residence, in a Member State in which it actually carries on business

A payment institution that has a waiver will still be subject to the PSD's conduct of business requirements.

Belgium has implemented this provision on waivers. We are not aware of other Member States' national legislation on waivers.

- ***In the Member States, is a payment service in which a payment institution grants credit in relation to payment service prevalent? If so, could you give some examples to show how those payment institutions provide such service?***

Yes.

E.g., a situation whereby a credit institution grants overdraft facilities on a payment account of a payment service user. This means that the payment service user is allowed "to go below zero" on its payment account, what would qualify as the provision of a payment service in relation to a credit.

E.g., a revolving credit in relation to a credit card.

- ***In the Member States, are payment institutions and electronic money institutions regulated to deal with systemic risks (taking into account the amount of payment transactions executed by them)?***

Payment institutions and e-money institutions are subject to rules on oversight of the ECB and of National Central Banks (even though they are subject to an extremely low level of risk which does not pose a systemic risk to the financial system).

- ***Are customer loyalty programs (free-of-charge point programs including the mileage program) regulated? Would the regulation treat the activity differently if customers are able to exchange the points with other payment instruments or cash? Are you aware that the Committee is considering to introduce a regulation on those programs in future, or do you know if any Member States are considering an introduction of such regulation?***

They are not regulated as such by the PSD or the e-money Directive.

Customer loyalty systems where "points" are earned via purchases of products or services and that cannot be purchased against cash payment will not require a payment services or e-money license if properly structured. In order to avoid the definition of e-money it is critically important to prohibit the purchase of extra points or the transfer of points / miles from one account to another account, because one of the key definitions of e-money is that the e-money is issued against payment of a cash amount. Points earned by purchasing airline tickets or other items is nothing but a form of a rebate granted by the participating merchant / airline.

However, the qualification of customer loyalty systems as "e-money" (or as a payment service) may differ from one Member State to another.

***

Yours sincerely,

Pierre Berger
Partner
+3232134040
Pierre.berger@bakermckenzie.com

Olivier Van den broeke
Associate
+322134040
Olivier.vandenbroeke@bakermckenzie.com

PAYMENT SERVICES - UNITED KINGDOM

1. Overview over payment and settlement related regulations (including matters not relating to laws and regulations)

1.1 Background to Regulations

(a) Payment Service Regulations

The regime originates from a European Community law; the Payment Services Directive ("**PSD**"). The aim of the PSD is to foster a single market in retail payment services across the European Economic Area ("**EEA**") by:

- removing barriers to entry and ensuring fair market access to enhance competition in payment services; and
- establishing the same set of rules across the EEA on information requirements and other rights and obligations that will be applicable to many payment services transactions in the EEA.

The Payment Services Regulations 2009 ("**PSRs**") and parts of the FCA Handbook implement the PSD in the UK. In general, these require payment service providers to be either authorised or registered by the FCA and to comply with certain rules about providing payment services, including specific requirements concerning payment transactions.

The PSRs do the following:

- Introduce an authorisation and prudential regime for payment service providers that are not banks, building societies or e-money issuers (and so already authorised or certificated by the FCA under a different regulatory regime). Businesses authorised under the PSRs are known as authorised payment institutions ("**authorised PIs**"). Authorised PIs can passport their services to other EEA States – in other words, because of their UK authorisation, they have the right to establish or provide services across the EEA.
- Allow payment service providers operating beneath a certain average monthly turnover threshold to be registered instead of obtaining authorisation (regulation 13). Such small payment institutions (small PIs) are unable to passport.
- Exempt certain payment service providers (for example, banks, electronic money institutions (authorised EMIs and small EMIs) from authorisation/registration requirements.
- Set out conduct of business requirements. In this context, this means requirements for information to be provided to payment service users, and specific rules on the respective rights and obligations of payment service users and providers. These requirements were applicable to all payment service providers with effect from 1 November 2009, whether they are payment institutions, banks, building societies, e-money issuers or any other category.
- Stipulate that rules governing access to payment systems should be non-discriminatory, subject to certain exemptions. This is aimed at supporting competition among payment service providers.

(b) E-Money Regulations

The Electronic Money Regulations ("**EMRs**") regulatory regime implements the Second Electronic Money Directive, which was adopted by the European Parliament and the Council of the European Union in September 2009.

(c) The FCA Handbook:

- sets out complaints handling procedures that PIs must have in place;
- establishes the right of certain customers to complain to the Financial Ombudsman Service ("**FOS**")[1];
- sets out the FCA's policy and procedures for taking decisions relating to enforcement action and when setting penalties; and
- contains rules on application, the FCA's ongoing fees, and FOS levies.

2. Overview of the Payment Services Regulations 2009

2.1 The PSRs were enacted in the UK in 2009. Below is a summary of the provisions contained in the Regulations.

(a) Part 1 - Introductory Provisions

This section contains exemptions from the PSRs for certain bodies (Reg 3).

(b) Part 2 - Registration

This section contains the application process and conditions for authorisation as a payment institution (Regs 5 and 6), as well as the regulations for varying permissions (Reg 8) and cancelling authorisation (Reg 9).

This section also contains the registration process for small payment institutions (Regs 12-15) and the duty of all payment institutions to notify changes (Reg 16).

(c) Part 3 - Authorised Payment Institutions

This section contains the capital requirements for authorised payment institutions (Reg 12), their safeguarding requirements (reg 19), their accounting and statutory audit requirements (Reg 20) and outsourcing and record keeping requirements (Regs 21 and 22).

This section also contains regulations regarding the exercise of passport rights by authorised PIs (Regs 23-26).

(d) Part 4 - Provisions applicable to Authorised Payment Institutions and Small Payment Institutions

This section contains provisions on additional activities of payment institutions (Reg 27), the use of agents (Reg 29) and the duty to notify the FCA of a change in the institution's circumstance (Reg 32).

(e) Part 5 - Information requirements for Payment Services

This section contains provisions on the application and disapplication of Part 5 (Regs 33-35).

[1] The FOS is a statutory, informal dispute-resolution service, established under FSMA and operationally independent of the FCA. It operates as an alternative to the civil courts. Its role is to resolve disputes between individuals, micro-enterprises, small charities and trusts, and financial services firms quickly, without taking sides and with minimum formality, on the basis of what is fair and reasonable in the circumstances of each case. In considering what is fair and reasonable, the FOS takes into account the relevant law, regulations, regulators' rules, guidance and standards, relevant codes of practice (such as the Remittances Customer Charter) and, where appropriate, what it considers to have been good industry practice at the relevant time.

This section also contains the information required in relation to single payment service contracts (Regs 36-39) and regulations relating to framework contracts (Regs 40-46).

(f) Part 6 - Rights and obligations in relation to the Provision of Payment Services

This section contains provisions on the application and disapplication of Part 6 (Reg 51-53) and regulations on charges (Reg 54).

This section also contains regulations on the authorisation of payment transactions (Regs 55-64) including consent requirements, the obligations placed on the payment service user and payment service provider in relation to payment instruments and the payer's liability for unauthorised payment transactions.

This section further contains regulations relating to the execution of payment transactions (Regs 65-68) including the requirements for receipt and refusal of payment orders. It also contains the regulations regarding execution time and value date (Regs 69-73).

Finally, this section contains the provisions on liability (Regs 74-79), including liability of the payment service provider for charges and interest (Reg 77), the right of recourse (Reg 78) and liability regarding non-execution or defective execution (Regs 75-76).

(g) Part 7 - The Authority

This section contains the regulations on the functions of the FCA (Reg 80) and their supervision and enforcement powers (Regs 81-91). The ssupervision powers of the FCA listed in this section include reporting requirements (Reg 82), the power to publicly censure (Reg 84), the power to impose financial penalties (Reg 85), the FCA's powers relating to injunctions (Reg 87) and powers relating to restitution orders (Reg 90).

(h) Part 8 - Access to Payment Systems

This section includes regulations on the application of Part 8 (Reg 96) and prohibitions on restrictive rules on access to payment systems (Reg 97).

This section also contains regulations on the powers of the CMA to investigate (Reg 98), the CMA power to require information (Reg 99), privileged communications (Reg 101) and the power of the CMA to impose financial penalties (Reg 105).

(i) Part 9 - General

This section contains regulations relating to criminal offences including the prohibition on provision of payment services by persons other than payment service providers (Reg 110); false claims to be a payment service provider (Reg 111); and defences (Reg 112).

This section also contain regulations regarding the duties of the FCA, the Commissioners and the CMA to co-operate and exchange information (Reg 119), the right of these authorities to bring actions (Reg 120) and regulations relating to transitional provisions (Regs 121-125B).

(j) Schedule 1 - Payment Services

Part 1 of this Schedule lists the services that are designated as 'payment services'.

Part 2 of this Schedule lists the activities which are deemed not to constitute payment services.

(k) Schedule 2 - Information to be included in or with an application for authorisation

This Schedule contains the information to be provided by the payment institutions when applying to become an authorised PI.

(l) Schedule 3 - Capital Requirements

This Schedule contains the initial capital requirements for payment institutions (Part 1) and requirements regarding own funds (Part 2).

(m) Schedule 4 - Prior general information for framework contracts

This Schedule supplements the requirements for framework contracts in Regs 40-46 (referred to above).

(n) Schedule 4A - Credit Agreements

This Schedule contains prohibitions and restrictions on the entry into credit agreements (Part 1) and the procedures and appeals against these restrictions (Part 2).

3. Overview of the E-Money Regulations 2011

3.1 The EMRs were enacted in the UK in 2011. Below is a summary of the provisions contained in the Regulations.

(a) Part 1 - Introductory Provisions

This section contains the definition of e-money (Reg 2) and the e-money exclusions (Reg 3).

(b) Part 2 - Registration

This section contains the application process and the conditions for authorisation as an e-money institution (Regs 5-7), the regulations relating to variation of the authorisation (Reg 8) and the cancellation of authorisation (Reg 11).

This section also contains the requirements for registration as a small electronic money institution (Regs 12-16) including the conditions for registration (Reg 13).

Finally, the section also contains the duty placed on institutions to notify changes in their firm (Reg 17) and provisions relating to e-money institutions acting without permission (Reg 18).

(c) Part 3 - Prudential Supervision and Passporting

This section contains the capital requirements for e-money institutions (Reg 19), as well as their safeguarding requirements (Regs 20-23), requirements regarding accounting and statutory audits (Reg 25) and provisions relating to outsourcing and record keeping (Regs 26-27).

This section also contains regulations regarding the exercise of passport rights by e-money institutions (Regs 28-31).

(d) Part 4 - Additional Activities and use of Distributors and Agents

This section contains regulations regarding additional activities of e-money institutions (Reg 32), their use of distributors and agents (Reg 33-35) and their duty to notify changes in circumstances regarding distributors and agents (Reg 37).

(e) Part 5 - Issue and Redeemability of E-Money

This section includes requirements on the issuance and redeemability of E-Money (reg 39), conditions for the redemption of e-money (Reg 40), the amount of redemption (Reg 42) and regulations relating to the termination of a contract (Reg 46).

(f) Part 6 - The Authority

This section contains provisions relating to the functions of the FCA (Reg 47) and their supervision and enforcement powers (Reg 48-58) including reporting requirements (Reg 49), their power to publicly censure (Reg 50), their power to issue financial penalties (Reg 51), their power relating to injunctions (Reg 54) and their powers relating to restitution (Reg 55-57).

(g) Part 7 - General

This section sets out criminal offences including the prohibition on issuing e-money by persons other than e-money issuers (Reg 63), false claims to be an e-money issuer (Reg 64) and defences (Reg 65).

This section also contains regulations relating to the duty of the FCA and Commissioners of HM Revenue and Customs to co-operate and exchange information (Reg 71) and their right to bring actions (Regs 72 and 72). There are also provisions in this section relating to transitional provisions (Regs 74-78).

(h) Schedule 1 - Information to be included in or with an application for authorisation

This Schedule contains the information to be provided by the e-money institutions when applying to become an authorised EMI.

(i) Schedule 2 - Capital Requirements

This Schedule contains the initial capital requirements for payment institutions (Part 1) and requirements regarding own funds (Part 2).

(j) Schedule 2A - Credit Agreements

This Schedule contains prohibitions and restrictions on the entry into credit agreements (Part 1) and the procedures and appeals against these restrictions (Part 2).

4. Payment and settlement services

4.1 Types of regulated payment services in the UK

(a) Payment Services

The payment services covered by the PSRs are listed in Part 1 of Schedule 1. These are set out below, along with some examples of the sort of payment services expected to fall within the scope of each.

- Services enabling cash to be placed on a payment account and all of the operations required for operating a payment account.(e.g. Payments of cash into a payment account over the counter and through an ATM.)

- Services enabling cash withdrawals from a payment account and all of the operations required for operating a payment account.(e.g. Withdrawals of cash from payment accounts, for example through an ATM or over the counter)

- Execution of the following types of payment transaction:

  - direct debits, including one-off direct debits;

  - payment transactions executed through a payment card or a similar device;

  - credit transfers, including standing orders.

    (e.g. Transfers of funds with the user's payment service provider or with another payment service provider; direct debits (including one-off direct debits). N.B. Acting as a direct debit originator would not, of itself, constitute the provision of a payment service. Also, transferring e-money and credit transfers, such as standing orders, BACS or CHAPS payments).

- Execution of the following types of payment transaction where the funds are covered by a credit line for a payment service user:

  - direct debits, including one-off direct debits;

  - payment transactions through a payment card or a similar device;

  - credit transfers, including standing orders.

    (e.g. Direct debits using overdraft facilities; card payments; credit transfers using overdraft facilities)

- Issuing payment instruments or acquiring payment transactions. (e.g. Card issuing (other than mere technical service providers who do not come into possession of funds being transferred) and card merchant acquiring services (rather than merchants themselves)).

- Money remittance (e.g. Money transfer/remittances that do not involve payment accounts)

- Execution of payment transactions where the consent of the payer to execute a payment transaction is given by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or network operator, acting only as an intermediary between the payment service user and the supplier of the goods and services (e.g. Mobile or fixed phone payments, where the payment is made from the phone itself rather than the phone being used as an authentication tool to send a payment order to another payment service provider. Also payments made from handheld devices (for example, BlackBerry)).

4.2 "Payment Account" v "deposit" v "e-money"

Articles 9AB and 9L of the Financial Services and Markets Act 2000 (Regulated Activities Order) 2001 ("**RAO**") provide that funds received by payment institutions from payment services users with a view to the provision of payment services shall constitute neither deposits nor electronic money.

As an authorised payment institution, any funds you hold must only be used in relation to payment transactions (see regulation 28 of the PSRs). A "payment transaction" for these purposes is defined in regulation 2 of the PSRs as meaning "*an act, initiated by the payer or payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and payee*". The fact that a payment account operated by a payment institution can only be used for payment transactions distinguishes it from a deposit. A deposit can nevertheless be a form of payment account and for guidance on what constitutes a deposit for the purposes of the regulated activity of "accepting deposits."

A payment institution is not prohibited from paying interest on a payment account but such interest cannot be paid from funds received from customers. More generally, if a payment institution were to offer savings facilities to its customers in the accounts it provides, in our view it would be holding funds not simply in relation to payment transactions and so would be in breach of regulation 28 of the PSRs.

(a) E-Money

Regulation 2 of the EMRs defines e-money as monetary value represented by a claim on the issuer that is:

- stored electronically, including magnetically;
- issued on receipt of funds for the purpose of making payment transactions;
- accepted as a means of payment by persons other than the issuer; and
- is not excluded by regulation 3 of the EMRs.

Examples of e-money include prepaid cards that can be used to pay for goods at a range of retailers, or virtual purses that can be used to pay for goods or services online.

(b) Exemptions

(i) Payment Services

Schedule 1 Part 2 to the PSRs contains a list of services that are not considered payment services and corresponds with Article 3 of the PSD:

- Payment transactions executed wholly in cash and directly between the payer and the payee, without any intermediary intervention.
- Payment transactions between the payer and the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee.
- The professional physical transport of banknotes and coins, including their collection, processing and delivery.
- Payment transactions consisting of non-professional cash collection and delivery as part of a not-for-profit or charitable activity.
- Services where cash is provided by the payee to the payer as part of a payment transaction for the purchase of goods or services following an explicit request by the payer immediately before the execution of the payment transaction.
- Money exchange business consisting of cash-to-cash operations where the funds are not held on a payment account.
- Payment transactions based on any of the following documents drawn on the payment service provider with a view to placing funds at the disposal of the payee-
    - paper cheques of any kind, including travellers' cheques;
    - bankers' drafts;
    - paper-based vouchers;

- paper postal orders.

- Payment transactions carried out within a payment or securities settlement system between payment services providers and settlement agents, central counterparties, clearing houses, central banks or other participants in the system.

- Payment transactions related to securities asset servicing, including dividends, income or other distributions, or redemption or sale, carried out by persons referred to in sub-paragraph (h) or by investment firms, credit institutions, collective investment undertakings or asset management companies providing investment services or by any other entities allowed to have the custody of financial instruments

- Services provided by technical service providers, which support the provision of payment services, without the provider entering at any time into possession of the funds to be transferred, including-

  - the processing and storage of data;

  - trust and privacy protection services;

  - data and entity authentication;

  - information technology;

  - communication network provision; and

  - the provision and maintenance of terminals and devices used for payment services.

- Services based on instruments that can be used to acquire goods or services only-

  - in or on the issuer's premises; or

  - under a commercial agreement with the issuer, either within a limited network of service providers or for a limited range of goods or services,

and for these purposes the "issuer" is the person who issues the instrument in question.

- Payment transactions executed by means of any telecommunication, digital or IT device, where the goods or services purchased are delivered to and are to be used through a telecommunication, digital or IT device, provided that the telecommunication, digital or IT operator does not act only as an intermediary between the payment service user and the supplier of the goods and services.

- Payment transactions carried out between payment service providers, or their agents or branches, for their own account.

- Payment transactions between a parent undertaking and its subsidiary or between subsidiaries of the same parent undertaking, without any intermediary intervention by a payment service provider other than an undertaking belonging to the same group.

- Services by providers to withdraw cash by means of automated teller machines acting on behalf of one or more card issuers, which are not party to the framework contract with the customer withdrawing money from a payment account, where no other payment service is conducted by the provider.

Guidance on these exemptions is contained in Chapter 15 of the Perimeter Guidance Manual ("**PERG**") in the FCA Handbook.

For example, on the question as to whether payment transactions between the payer and the payee through a commercial agent authorised only to receive payment of the costs of goods and services on behalf of the payee would be regulated, such an activity could fall outside the scope of the PSRs. This is on the basis of the exclusion that "*payment transactions between the payer and the payee through a commercial agent authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payer or the payee.*" Key considerations in this case would be whether the agent is in fact authorised to negotiate or conclude the sale or purchase of goods.

Further, there is guidance at Question 25 of PERG 15 states the following:

We are a bill payment firm. Do the PSD regulations apply to us?

Not in our view where you receive payment on behalf of the payee so that your receipt constitutes settlement of the payer's debt to the payee. By contrast, if you provide a remittance service which does not involve receipt on behalf of the payee and corresponds to the definition of "money remittance" in regulation 2, you will be providing a money remittance service.

This suggests that where receipt of payment by a third party (such as a commercial agent) extinguishes the debt owed by the payer to the payee then such a transaction will not constitute the payment service of money remittance. In any event, in all cases, it is important to assess the flow of funds and roles of the parties in order to determine whether a payment service is being performed and whether an exclusion may be available.

(ii) E-Money

The EMRs have two express exclusions:

- the first covers monetary value stored on instruments that may be used to purchase goods and services only in the issuer's premises or within a limited network of service providers or for a limited range of goods or services (regulation 3(a)); and
- the second covers monetary value used to make payment transactions executed by means of any telecommunication, digital or IT device where the goods or services are delivered to and used through such a device but only where the operator of the device does not act only as an intermediary between the user and the supplier (regulation 3(b)).

(iii) Specific questions

Question: The Japanese Payment Services Act does not have the definition of "Funds Transfer Service" (which is defined by case law). Do European countries' regulations have such definition?

Answer: Yes, see above which lists the regulated payment services in the PSRs i.e. money remittance at 4.1(f) above.

Question: How are business activities identified to which payment and settlement regulation apply?

Answer: By analysing the payment flows und underlying agreements and subsuming under the definitions. The law takes a functional approach focusing on the types of **activity carried** on as opposed to the types of institution involved in the activity. Therefore, organisations such as mobile network operators, outsourcing companies and technology companies may all be subject to regulation if the substantively carry out a regulated activity.

Question: How do European countries regulate payment and settlement services (i.e. what are the criteria by which the regulations applied to payment and settlement services are varied)?

Answer: As indicated, laws define the specific types of activity that are subject to regulation. If such an activity is carried on and no exemption is available, then the regulation will apply. Differentiating criteria are:

- are payment accounts used?
- pull or push transaction?
- standing order?
- is a payment card used?
- is credit granted?
- is a digital device used?

The approach is relatively flexible with the scope of laws typically being reviewed on a periodic basis, in particular, to keep abreast of technological developments.

Question: Are the payment and settlement services and deposit are permitted to banks exclusively?

Answer: No, but typically banks will provide such payment services. They do not require a separate payment services licence. However these activities can be carried on by parties other than banks.

Question: Do the regulations vary based upon the prepaid payment instrument (ex. prepaid cards), immediate payment instrument (ex. debit cards) and post payment instrument (ex. credit cards)?

Answer: Yes, as different characteristics of the product will influence its categorisation for regulatory purposes. The regulations applying to e-money (i.e. typically pre-paid) differ from those that apply to payment services. Payment cards such as debit cards and credit cards are subject to regulation under the PSRs.

Question: Is the free of charge point service regulated? If so how? In addition, do such regulations on free of charge point services vary based upon whether such point can be exchanged with another payment instruments or cash?

Answer: Points / loyalty schemes can fall within the scope of regulation, particularly of e-money. Schemes where "points" are earned via purchases of products or services and cannot be purchased against cash payment will not require a payment or services or e-money license if properly structured. In order to avoid the definition of e-money it is critically important to prohibit the purchase of extra points or the transfer of points / miles from one account to another account, because one of the key definitions of e-money is that the e-money is issued against payment of a cash amount. The key issue is whether points have a particular monetary value as opposed to being redeemed for a service or product for which a specific monetary value has not been attributed. Each such scheme must be individually assessed.

We are not aware of any proposed legislative changes which will specifically regulate such points/loyalty schemes from a financial services licensing perspective.

That being said, schemes which prima facie constitute e-money and which presently rely on the "limited network" exemption may find it difficult to do so in the near furture due to the changes proposed under PSD 2 (see EU comments above) and the likely consequential changes to the Second Electronic Money Directive which will follow.

Question: Under the Japanese Payment Services Act, service providers being registered under the Act are regulated by uniform regulations, such as assets protection obligations (ex. requirement of cash deposit as performance guarantee, etc.), and regulations on performance/activities (ex. requirement of business structure, information protection system/structure, and information disclosure to clients, etc.). Do the regulations vary based on the services in European countries?

Answer: Yes, regulations vary, too, in particular with respect to initial capital requirements and adequate capital. Otherwise, regulations are similar. To some extent, payment services providers have a certain amount of discretion regarding their business organizations depending on the risk profile of the business.

(iv) Comparison with Japanese Payment Services

The table below compares the Japanese Payment Services with payment services found in the UK. All of the services listed below are available and used in the UK.

Please note: Although statistics for payment services are published by the Payments Council and the UK Cards Association annually, we are not a member of these bodies and therefore cannot access this information.

Japan	**UK**
Exchange Transactions by banks or funds transfer service providers	Corresponds to money remittance business assuming the transactions are non-account based. Two of the biggest money remittance companies in the UK are Western Union and MoneyGram. According to their website, Western Union Holdings allows customers to send and receive money anywhere in the world in person, online or by phone. They also offer bill payment services for customers via a variety of methods. Western Union's money transfer and bill payment services are also complemented by a variety of prepaid services, including reloadable prepaid, gift and phone cards, and money orders. According to their website, Moneygram International Limited is a money transfer company and is the second largest provider of money transfers in the world. MoneyGram allows customers to send and receive money from or to over 200 countries. Western Union is listed in the FCA's Payment Services Firm register as having permission to carry on cash placement services on a payment account; cash withdrawal services on a payment account; executing payment transactions (no credit line); executing payment transactions (credit line); issuing instruments/acquiring transactions; money remittance and executing payment transactions via telecoms etc. MoneyGram is listed in the FCA's Payment Services Firm register as having permission to carry on money remittance.
Prepaid payment instruments (self-provided or third party-provided; paper-based, IC-based or server-based)	Corresponds to electronic money business. Self-provided instruments where the issuing and accepting party are the same legal person are not regulated. Third party-provided instruments are

	considered e-money. Paper-based instruments are exempt from regulation, whereas IC-based or server-based instruments fall under the definition of e-money if accepted by another person than the issuer. There are currently 66 firms registered on the E-Money Register. This means that there are 66 (non-banks) which are authorised in the UK to issue e-money (and perform payment services). Google Wallet is an example of e-money business in the UK. Google Wallet is a mobile payment system developed by Google that allows its users to store debit cards, credit cards, loyalty cards, and gift cards among other things, as well as redeeming sales promotions on their mobile phone. Google Wallet is listed on the E-Money Register as carrying out services enabling cash placement on a payment account; services enabling cash withdrawals from a payment account; execution of payment transactions (not covered by a credit line); execution of payment transactions (covered by a credit line); issuing payment instruments or acquiring payment transactions; money remittance; execution of payment transactions via telecoms etc; and issuing e-money.
Credit card settlements (including issuing, acquiring and international credit card brand services)	Issuing credit cards and performing merchant acquiring services are regulated under the UK's PSRs. An example of a company carrying out the issuing of credit cards in the UK is American Express as well as many UK banks. American Express issue their own debit and credit cards to UK customers directly. American Express are listed in the Payment Services Firm register as having permission to issue instruments and carry out acquiring transactions. An example of a company performing merchant acquiring services in the UK is World Pay. World Pay are the UK's leading payment provider. They help many small and medium sized businesses to get started and set up card systems. World Pay are listed in the Payment Services Firm register as having permission to execute payment transactions (no credit line); execute payment transactions (credit line); issue instruments and acquiring transactions and money remittance.
Post-paid type e-money (settlement by credit cards)	This could involve the issue of charge or credit cards.
Payment receiving agency, collection agency	This is likely to form one part of money remittance service assuming the transactions are non-account

	based.
Account transfer agency	This is likely to include money remittance business assuming the transactions are non-account based.
Fund transfer agency	This is likely to include to money remittance business, assuming the transactions are non-account based.
Settlement agency	This is likely to involve money remittance business, assuming the transactions are non-account based.
Cash-on-delivery	Cash transactions are typically exempt
Escrow services	Depending on the use of a payment account this corresponds to payment transaction or money remittance business.

4.3 Regulation in the UK

(a) Licensing scheme, requirements and regulated activities

(i) Payment Services

A UK firm that provides payment services by way of business in the UK needs to apply to the FCA to become either an authorised payment institution ("**authorised PI**") or a small payment institution ("**small PI**"); unless it is already another type of payment service provider or is exempt.

Being a small PI is an option available to businesses whose average turnover in payment transactions does not exceed €3 million per month. The registration process is cheaper and simpler than authorisation and has no ongoing capital requirements, but there are no passporting rights for small PIs. The conduct of business requirements still apply, as does access for small PIs' eligible customers to the FOS.

Agents can be appointed by a PI (the principal) to provide payment services on the principal's behalf. The principal accepts responsibility for the actions of the agent and must make an application on the agent's behalf for inclusion on the Financial Services Register.

To become an authorised PI, an applicant must fulfil the following criteria:

- The application must provide all information requested by the FCA contained in Schedule 2 of the PSRs including:
  - ➢ A programme of operations setting out, in particular, the type of payment services envisaged (Sch 2 para 1 PSRs);
  - ➢ A business plan including a forecast budget calculation for the first three financial years which demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures to operate soundly (Sch 2 para 2 PSRs);
  - ➢ A description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of its participation in a national or international payment system (Sch 2 para 7 PSRs);

- The applicant must immediately before the time of authorisation hold the amount of initial capital required (Reg 6(3) and Part 1 Sch 3 PSRs):

  - Money remittance - €20,000;

  - Execution of payment transactions where payer's consent for execution is given via a telecommunication, digital or IT device and payment is made to the telecommunication, IT system or network operator acting only as anintermediary between the payment service user and the supplier of the goods or services - €50,000;

  - Payment institutions providing other services, that is those covered in Schedule 1 Part 1(1)(a) to (1)(e) of the PSRs - €125,000.

  There are also ongoing capital requirements that the payment institution will have to comply with. The initial capital requirements depends of the activities to be performed by the institution under its payment service licence. The difference reflects the varying risks associated with the activities.

- The applicant must be a body corporate constituted under the law of a part of the United Kingdom having (s6(4) PSRs) —

  - its head office, and

  - if it has a registered office, that office, in the United Kingdom.

- The applicant must satisfy the FCA that, taking into account the need to ensure the sound and prudent conduct of the affairs of the institution, it has (s6(5) PSRs)—

  - robust governance arrangements for its payment service business, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;

  - effective procedures to identify, manage, monitor and report any risks to which it might be exposed;

  - adequate internal control mechanisms, including sound administrative, risk management and accounting procedures,

  which are comprehensive and proportionate to the nature, scale and complexity of the payment services to be provided by the institution.

- The applicant must satisfy the FCA that (s6(6) PSRs)—

  - any persons having a qualifying holding[2] in it are fit and proper persons having regard to the need to ensure the sound and prudent conduct of the affairs of an authorised payment institution;

  - the directors and persons responsible for the management of the institution and, where relevant, the persons responsible for the management of payment services, are of good repute and possess appropriate knowledge and experience to provide payment services;

[2] A "qualifying holding" is defined in the PSRs by reference to Article 4(11) of the Banking Consolidation Directive (BCD). The definition in the BCD is a 'direct or indirect holding in an undertaking which represents 10% or more of the capital or of the voting rights or which makes it possible to exercise a significant influence over the management of that undertaking'. The FCA refers to persons/entities with a qualifying holding as "controllers."

- ➢ it has a business plan (including, for the first three years, a forecast budget calculation) under which appropriate and proportionate systems, resources and procedures will be employed by the institution to operate soundly; and
  - ➢ it has taken adequate measures for the purpose of safeguarding payment service users' funds in accordance with regulation 19 of the PSRs.

- The applicant must comply with a requirement of the Money Laundering Regulations 2007 to be included in a register maintained under those Regulations where such a requirement applies to the applicant (s6(7) PSRs).

- If the applicant has close links with another person ("**CL**") the applicant must satisfy the Authority (s6(8) PSRs) —

  - ➢ that those links are not likely to prevent the Authority's effective supervision of the applicant; and
  - ➢ if it appears to the Authority that CL is subject to the laws, regulations or administrative provisions of a territory which is not an EEA State ("the foreign provisions"), that neither the foreign provisions, nor any deficiency in their enforcement, would prevent the Authority's effective supervision of the applicant.

- For the purposes of paragraph (g), an applicant has close links with CL if (s6(9) PSRs):

  - ➢ CL is a parent undertaking of the applicant;
  - ➢ CL is a subsidiary undertaking of the applicant;
  - ➢ CL is a parent undertaking of a subsidiary undertaking of the applicant;
  - ➢ CL is a subsidiary undertaking of a parent undertaking of the applicant;
  - ➢ CL owns or controls 20% or more of the voting rights or capital of the applicant; or
  - ➢ the applicant owns or controls 20% or more of the voting rights or capital of CL.

It is worth noting that authorised PIs and small PIs may, in addition to providing payment services, engage in the following activities (regulation 27 of the PSRs):

- the provision of operational and closely related ancillary services including ensuring the execution of payment transactions, foreign exchange services, safe-keeping activities and the storage and processing of data;
- the operation of payment systems; and
- business activities other than the provision of payment services, subject to any relevant Community or national law.

Further, authorised PIs and small PIs may grant credit in relation to the provision of payment services specificed in paragraph 1(d), (e) and (g) of Schedule 1 of the PSRs only if:

- such credit is ancillary and granted exclusively in connection with the execution of the payment transactions;
- such credit is not granted from the funds received or held for the purpose of executing payment transactions;

- in cases where credit in granted by an authorised PI exercising its passporting rights, there is an obligation upon the payment service user to repay the credit within a period not exceeding 12 months; and
- in relation to an authorised PI, in the opinion of the FCA the insitution's own funds are, and continue to be, adequate in light of the overall amount of credit granted.

(ii) Electronic Money

In general, a UK business or a UK branch of a business with its head office outside the EEA that intends to issue e-money (as defined in the EMRs) has to be either an authorised EMI or a small EMI or have Part 4A permission to issue e-money under the Financial Services and Markets Act 2000 ("**FSMA**"). In accordance with regulation 32 of the EMRs, EMIs are permitted to provide payment services without having to be separately authorised or registered under the PSRs.

Businesses whose total business activities are projected to generate average outstanding e-money that does not exceed €5m may apply to be registered as small EMIs. Small EMIs may provide unrelated payment services, but only on the same basis as a small payment institution; that is, the monthly average, over a period of 12 months, of the total amount of relevant payment transactions must not exceed €3m. Please note that the conditions fore registration are different from the conditions to be an authorised EMI. The registration process is cheaper and more straightforward than authorisation, but there are no passporting rights. Some small EMIs are subject to capital requirements and all are subject to the safeguarding and conduct of business requirements. Small EMIs can provide unrelated payment services but only if the average monthly total of payment transactions does not exceed €3m, on a rolling 12-month basis. Small EMIs must notify the FCA of the types of payment services they wish to provide.

To become an <u>authorised EMI</u>, an applicant must fulfil the criteria found in s6 of the EMRs. These criteria are set out below:

- The application must provide all information requested by the FCA contained in Schedule 1 of the EMRs including:
  - A programme of operations setting out, in particular, the type of payment services envisaged (Sch 1 para 1 EMR);
  - A business plan including a forecast budget calculation for the first three financial years which demonstrates that the applicant is able to employ appropriate and proportionate systems, resources and procedures to operate soundly (Sch 1 para 2 EMR);
  - A description of the applicant's structural organisation, including, where applicable, a description of the intended use of agents and branches and a description of outsourcing arrangements, and of its participation in a national or international payment system (Sch 1 para 7 EMR);
- The applicant must be either—
  - a body corporate constituted under the law of a part of the United Kingdom having—
    - its head office; and
    - if it has a registered office, that office,

    in the United Kingdom; or

- a body corporate which has a branch that is located in the United Kingdom and whose head office is situated in a territory that is outside the EEA.

- An applicant for authorisation as an electronic money institution must hold an amount of initial capital of at least €350,000.

  - Where the business activities of an applicant for registration as a small EMI generate average outstanding electronic money of €500,000 or more it must hold an amount of initial capital at least equal to 2% of the average outstanding electronic money of the institution. There is no initial capital requirement for small EMIs whose business activities generate (or are projected to generate) average outstanding e-money less than €500,000.

  - Where the applicant has not completed a sufficiently long period of business to calculate the amount of average outstanding electronic money for the purposes above, the applicant must make an estimate on the basis of projected outstanding electronic money as evidenced by its business plan, subject to any adjustments to that plan which are, or have been, required by the FCA.

- The applicant must satisfy the Authority that, taking into account the need to ensure the sound and prudent conduct of the affairs of the institution, it has—

  - robust governance arrangements for its electronic money issuance and payment service business, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility;

  - effective procedures to identify, manage, monitor and report any risks to which it might be exposed; and

  - adequate internal control mechanisms, including sound administrative, risk management and accounting procedures, which are comprehensive and proportionate to the nature, scale and complexity of electronic money to be issued and payment services to be provided by the institution.

- The applicant must satisfy the FCA that:

  - having regard to the need to ensure the sound and prudent conduct of the affairs of an authorised electronic money institution, any persons having a qualifying holding in the institution are fit and proper persons;

  - the directors and persons responsible for the management of its electronic money and payment services business are of good repute and possess appropriate knowledge and experience to issue electronic money and provide payment services;

  - it has a business plan (including for the first three years, a forecast budget calculation) under which appropriate and proportionate systems, resources and procedures will be employed by the institution to operate soundly;

  - it has taken adequate measures for the purpose of safeguarding electronic money holders' funds in accordance with Reg 20 of the EMRs.

- The applicant must comply with a requirement of the Money Laundering Regulations 2007 to be included in a register maintained under those Regulations where such a requirement applies to the applicant.

- If the applicant has close links with another person ("CL")the applicant must satisfy the FCA:

    - that those links are not likely to prevent the Authority's effective supervision of the applicant; and

    - if it appears to the Authority that CL is subject to the laws, regulations or administrative provisions of a territory which is not an EEA state ("the foreign provisions"), that neither the foreign provisions, nor any deficiency in their enforcement, would prevent the Authority's effective supervision of the applicant.

- For the purposes of paragraph (g), an applicant has close links with CL if—

    - CL is a parent undertaking of the applicant;

    - CL is a subsidiary undertaking of the applicant;

    - CL is a parent undertaking of a subsidiary undertaking of the applicant;

    - CL is a subsidiary undertaking of a parent undertaking of the applicant;

    - CL owns or controls 20% or more of the voting rights or capital of the applicant; or

    - the applicant owns or controls 20% or more of the voting rights or capital of CL.

Deposit-takers/banks and the PSRs/EMRs

For the avoidance of doubt, neither an authorised payment institution nor an authorised e-money issuer is permitted to carry on the regulated activity of "acceting deposits." In order to carry on the regulated activity of "accepting deposits" a firm would need to apply for permission under Part 4A of FSMA and not under the PSRs or EMRs.

Please note, however, that banks (i.e., entities which have permission to "accept deposits) can provide payment services without the need for authorisaiton/registration under the PSRs although these entities need to comply with the conduct of business requirements of the PSRs.

Banks (i.e., entities which have permission to "accept deposits") do not require authorisation or registration under the EMRs but if they propose to issue e-money they must have Part 4A permission under FSMA for the activity of issuing e-money. When issuing e-money, they are subject to the provisions on issuance and redeemability of e-money in the EMRs and to the relevant conduct of business requirements of the PSRs.

Other Entities and the PSRs/EMRs

The following persons do not need to apply for authorisation or registration under the EMRs but they must give the FCA notice if they issue or propose to issue e-money:

- the Post Office Limited;

- the Bank of England, the European Central Bank and the national central banks of EEA states other than the UK, when not acting in their capacity as a monetary authority or other public authority;

- government departments and local authorities when acting in their capacity as public authorities; and

- the National Savings Bank.

However, they will be subject to the conduct of business requirements of the EMRs, the conduct of business requirements of the PSRs for the payment service aspect (subject to the below), and they will have to report to the FCA their average outstanding e-money on a half-yearly basis. Certain customers will have access to the FOS.

The following can continue to provide payment services without the need for further authorisation or registration under the PSRs:

- banks (see comments above);
- building societies;
- EEA authorised PIs;
- authorised e-money institutions;
- small e-money institutions;
- Post Office Limited; and
- certain public bodies.

These entities must, however, comply with the conduct of business requirements of the PSRs. However, the following bodies are specifically exempt from the scope of the PSRs:

- credit unions;
- municipal banks; and
- The National Savings Bank.

Municipal banks and the National Savings Bank will also be exempt from the Banking: Conduct of Business sourcebook ("**BCOBS**") in the FCA Handbook. Municipal banks must nevertheless notify the FCA if they are providing, or propose to provide, payment services. Credit unions will be subject to BCOBS.

FCA's ability to impose conditions

PSRs

If the FCA decides to grant an application for authorisation/registration as a PI, it will give the applicant notice of that decision. This notice will specify the payment services for which approval has been granted, requirements (if applicable) and the date from which it takes effect. The PSRs allow the FCA to vary the types of payment services that a PI is ultimately approved to carry out from those requested in the application and to apply requirements to the PI as a condition of authorisation or registration that we consider appropriate (regulation 7). This may include requiring the firm to take a specified action, refrain from taking specified action (for example, not to deal with a particular category of customer) or relate to its relationship with its group or other members of its group. We may also specify the time that a requirement expires.

In accordance with regulation 7(4), where an applicant carries out non-payment services business and the FCA considers that the carrying on of this business will, or is likely to, impair its ability to supervise the firm or its financial soundness, the FCA can require the applicant firm to form a separate legal entity to perform payment services. In other words, the FCA may require that the applicant incorporate a separate UK company within the group whose sole activity will be the performance of payment services. Irrespective of the FCA's powers in this regard, in practice, it is not uncommon for applicant firms to incorporate a new company which will perform the payment services in order to ring-fence liability.

EMRs

If the FCA decide to grant an application for authorisation/regisrtration as an EMI, it will give the applicant notice of that decision, including, for authorised EMIs that wish to provide unrelated payment services, a direction on which capital calculation method they must use. The EMRs allow the FCA to include in the authorisation/registration a requirement for the EMI to take a specified action or refrain from taking specified action (for example, not to deal with a particular category of customer). The requirement may be imposed by reference to the person's relationship with its group or members of its group.

The FCA may also specify the time that a requirement expires (regulations 7 and 15 of the EMRs). For example, the FCA may require that the EMI refrains from providing specified unrelated payment services because we consider that the EMI does not have adequate systems and controls in place to manage the risks of the unrelated payment services.

5. On-going Requirements

A payment services institution and e-money institution are supervised by the FCA. Supervisory powers are similar to the powers that can be executed towards banks. The FCA takes a rigorous approach to the supervision of institutions that it regulates although supervision tends to be carried out remotely as opposed to onsite. The FCA has broad powers to required the production of information.

The FCA has the following supervisory powers:

(a) Capital Requirements Monitoring

The FCA monitors compliance of authorised PIs and EMIs with capital requirements by requiring the authorised PI and EMI to report the amount of capital they hold to the FCA annually. This annual report also requires authorised PIs and EMIs to provide information on the institution's safeguarding arrangements and the number of agents it has. The authorised PI or EMI must also confirm in the report that it has communicated any changes in these areas to the FCA. The reports are required within 30 days of a firm's year end.

In respect of small PIs and EMIs, the FCA require an annual report of both the volume and the value of transactions carried out. This information enables the FCA to make a report to the Commission (as they are required to do) and to ensure that the average monthly value of transactions undertaken by a firm has not risen above the level where it can remain a small PI or EMI. The FCA also require information on the number of agents a small PI or EMI has and whether it is voluntarily safeguarding payment service user funds. The report covers the calendar year from 1 January to 31 December, and must be submitted by the end of the following January.

(b) Complaints Monitoring and Redress

When the FCA receive a complaint alleging a breach of the conduct of business rules, the FCA consider whether it needs to take any supervisory action. In most cases, the FCA expect simply to make the complainant aware of the right to take a complaint to the Financial Ombudsman Service ("**FOS**") if they are not satisfied with the payment service provider's response. However, where a complaint to the FCA about an alleged breach is significant or suggests a systemic problem, the FCA are likely to follow up the complaint with supervisory action. This might involve, for example, a visit to the payment service provider concerned, or a request for a written explanation of the circumstances of the alleged breach.

Where themes arise from the analysis of complaints, indicating an industry-wide problem on certain issues, the FCA may undertake supervisory activity relating to that theme, such as visits to a number of firms to understand how they are managing the particular risk identified. Findings from such visits may lead both to specific action being required by certain firms and wider guidance being given to all firms.

In any case, where the FCA are not satisfied that a payment service provider or electronic money issuer has dealt appropriately with the causes of the non-compliance, they will discuss the matter with their Enforcement Division.

Please see comments below regarding the obligations on complaints handling.

(c) Powers to require information, appoint persons to carry out investigations and carry out skilled persons reports from Payment Service Providers

The FCA prefer to discharge its functions under the PSRs / EMRs by working in an open and cooperative relationship with payment service providers and EMIs. It looks to obtain information in the context of that relationship unless it appears that obtaining information in that way will not achieve the necessary results, in which case they will make use of their statutory powers. These include the following :

- The power to require specified information in connection with their responsibilities under the PSRs / EMRs;
- the power to require a report from a skilled person, nominated or approved by the FCA, on any matter that we require in connection with our responsibilities under the EMRs/PSRs. Further information on the FCA's policy on the use of skilled persons and the appointment and reporting process is contained in the Supervision manual of our Handbook ("**SUP**"), specifically at SUP 5.3 and 5.4

If it appears that there is a good reason for doing so, the FCA can appoint competent persons to conduct an investigation on its behalf.

(d) Power to impose penalties

The PSRs and EMRs allow the FCA to impose penalties and censures for breaches of the PSRs and EMRs and instigate criminal prosecutions against those who provide, or claim to provide, payment services or e-money services but are not authorised to do so (Regs 84 and 85 of the PSRs Regs 50 and 51 of the EMRs). They can also order firms to provide restitution to their customers. The FCA can cancel or place requirements on a PI’s or EMI's authorisation or registration where certain criteria, outlined in the PSRs or EMRs, are met.

In addition to serious breaches of the PSRs or EMRs, examples of the circumstances where the FCA may cancel an authorisation include, but are not limited to, persistent non-payment of fees and levies owed to the FCA, non-submission of an annual return and failing to provide the FCA with current contact information.

The FCA may also enforce EMIs’ and certain PIs financial crime obligations under other legislation, including FSMA, the Money Laundering Regulations 2007 and Schedule 7 to the Counter-Terrorism Act 2008.

6. On-going Requirements

(a) Ongoing Capital Requirements

PSRs

The PSRs establish capital requirements for authorised PIs. Under the PSRs, authorised PIs are required to hold a minimum amount of capital. Capital is required to be held as a buffer, absorbing both unexpected losses that arise while the firm is a going concern as well as the first losses when the firm is wound up. The parts of the PSRs that deal with the capital resources and requirements are regulations 6(3), 18, and Schedule 3. The term ‘capital resources’ describes what a firm holds as capital.

"Capital requirements" refers to the amount of capital that must be held by the firm for regulatory purposes. The capital requirements established by the PSRs are initial requirements which are a condition of authorisation and ongoing requirements. The items that may be used to meet the capital requirements are "qualifying items" (see below). The authorised PI must hold at all times the capital amounts required, in the manner specified. The capital requirements set out in the PSRs are expressed in euro, as they are in the PSD. It is expected that firms will hold sufficient capital to ensure that the capital requirements are met, even in the event of exchange rate fluctuations.

The full definition of each qualifying item can be found in paragraph 3 of Part 2 of Schedule 3 of the PSRs and include paid up share capital, reserves and profit and loss. Qualifying items are subject to deductions and limits. Firms must take these deductions and limits into account in good time, as they will apply immediately after authorisation.

Authorised PIs can undertake activities that are not related to providing payment services. These businesses are called 'hybrid' businesses. The PSRs do not impose any initial or ongoing capital requirements in relation to the business that does not involve payment services. Any other capital requirements imposed because of other legislation – for example, if the PI is undertaking an activity regulated under FSMA – have to be met separately and cumulatively. An authorised PI must not include in its capital calculations any item also included in the capital calculations of another authorised PI, credit institution, investment firm, asset management company or insurance undertaking within the same group. Also, where an authorised PI carries out activities other than providing payment services, it must not include in its capital calculation items used in carrying out the other activities.

As mentioned above, the initial capital requirement is one of the conditions to be met at the application stage in order for the authorised PI to become authorised by the FCA. The PSRs require that the authorised PI's capital must not at any time fall below the prescribed levels of initial capital for its business activity. The PSRs set out that the initial capital requirement of authorised PIs will be €20,000, €50,000 or €125,000 depending on the business activities carried out by the firm. Where more than one initial capital requirement applies to an authorised PI, it must hold the greater amount.

The ongoing capital requirement is to be met by the authorised PI's capital resources using "qualifying items" (as defined in the PSRs). The ongoing capital held must not fall below the level of the initial capital requirement for the services provided.

EMRs

Under the EMRs, the ongoing capital (own funds) requirement is to be met by the EMI's capital resources using certain "qualifying items" as set out below. The ongoing capital held must not fall below the level of the initial capital requirement for the services provided (see above).

An authorised EMI has to work out its ongoing capital requirements using method D under the EMRs. Small EMIs subject to an initial 2% capital requirement must continue to meet this on an ongoing basis unless their level of business falls below the threshold.

An authorised EMI chooses to provide unrelated payment services it must meet separate and additional ongoing capital requirements for the unrelated payment services part of the business. The authorised EMI does not have to meet any additional initial capital requirements for the unrelated payment services. The ongoing capital requirements for unrelated payment services are laid out in paragraph 13(a) of Schedule 2 to the EMRs. There are three ways of calculating the ongoing capital requirement for unrelated payment services: methods A, B and C. Authorised EMIs that provide unrelated payment services are asked to indicate which calculation method they wish to use. The FCA will direct (based on the FCA's evaluation of the authorised EMI) which method is to be used, taking into account the authorised EMI's preference.

Small EMIs are allowed to provide payments services not related to the issuance of e-money on the same basis as a small payment institution. There are no initial or ongoing capital requirements for small EMIs in relation to their unrelated payment services business.

Qualifying items to be used to meet the initial capital requirement are paid-up capital (including share premium account but excluding cumulative preference shares); reserves; and profit/loss. The EMRs also set out deductions that must be made from capital and limits on qualifying items, which are set out in details in the EMRs.

The ongoing capital requirement is to be met by the EMI's capital resources using qualifying items. Authorised EMIs and small EMIs with capital requirements work out ongoing capital requirements using method D for their e-money business and related payment services. Authorised EMIs that also provides unrelated payment services must work out their cumulative ongoing capital requirements using either methods A, B or C (see EMRs for further detail. The ongoing capital held must not fall below the level of €350,000.

(b) Information required from auditors

The PSRs and EMRs impose an obligation on an auditor of an authorised PI or EMI to report certain matters to the FCA that they have become aware of in their capacity as auditor of that PI or EMI. For example, if the auditor reasonably believes that there is or has been a contravention of any of the requirements of the PSRs or EMRs, they must report it to the FCA. On receipt of such information, the FCA will review and follow up with the firm and/or the auditors as appropriate.

(c) Obligation to notify the FCA of certain matters.

The PSRs contain requirements in relation to notifications of changes in specific circumstances, as well as a general requirement in regulation 32 of the PSRs. The general requirement is that where it becomes apparent to a PI that there is, or is likely to be, a significant change in circumstances, which is relevant to its fulfilment of the conditions for authorisation or registration, it must provide the FCA with details of the change without undue delay. Regulation 32 also requires that in the case of a substantial change which has not yet taken place, the PI must provide details of the change in good time before the change takes place. A 'substantial change' is, in our view, one that could impact on either the firm's ability to meet the conditions for remaining authorised or registered, or the way we would supervise the firm.

The EMRs contain requirements in relation to notifications of specific changes in circumstances, as well as a general requirement in regulation 37. The general requirement is that an EMI must provide the FCA with details without undue delay where it becomes apparent that there is, or is likely to be, a significant change in circumstances that is relevant to the matters listed below.

As such, PIs and EMIs are required to notify the FCA of such matters as changes to its name, address, qualifying holdings, directors, the fitness and property of relevant individual such as directors and significant changes to their business operations.

7. Client Protection Scheme - Safeguarding

(a) Payment Services

All authorised PIs are required to comply with the safeguarding requirements in Regulation 19 of the PSRs. Small PIs can choose to comply with safeguarding requirements in order to offer the same protections over customer funds as authorised PIs must provide. If a small PI does choose to safeguard it will need to apply the same level of protections as are expected of an authorised PI.

The PSRs impose safeguarding requirements to protect customer funds received for the provision of a payment service where they are held by a PI overnight or longer. They do this by ensuring that those funds are either segregated from the PI’s working capital and other funds, or are covered by an appropriate insurance policy or third party guarantee.

The requirement to safeguard applies to "relevant funds". These are sums received:

- from, or for the benefit of, a payment service user for the execution of a payment transaction; and
- from a payment service provider for the execution of a payment transaction on behalf of a payment service user.

This means that safeguarding extends to funds that are not received directly from a payment service user, but includes, for example, funds received by a PI from another payment service provider for the PI’s payment service user. Funds relating to a particular payment transaction only need to be safeguarded if they exceed £50 (in which case the full amount must be safeguarded, not just the amount by which the funds exceed the £50 threshold). PIs may, however, choose to safeguard amounts beneath this threshold, in which case the insolvency protections will apply.

Some PIs also receive funds from the public in respect of other services. Examples include, a foreign exchange business that also provides money transmission services, or a telecommunications network operator which receives funds from the public both for the provision of its own services (for example airtime), and for onwards transmission to third parties. Such ‘hybrid’ businesses are only required to safeguard the funds received for the execution of a payment transaction. However, sometimes such hybrid businesses will not know the precise portion of customer funds attributable to the payment transaction and to the non-payment service provided, or the amount may be variable. In these circumstances, a PI may make a reasonable estimate on the basis of relevant historical data of the portion that is attributable to the execution of the payment transaction and so must be safeguarded. The firm would, if asked, need to supply the FCA with evidence that the proportion actually safeguarded was representative. Relevant data might include the portion generally attributable to payment transactions by the customer in question or by similar customers generally.

In the FCA's view, a PI that is carrying out a foreign exchange transaction independently from its payment services (see further Question 12 in PERG 15.2) does not need to safeguard funds received for the purpose of the foreign exchange transaction. Indeed, where a PI is using the segregation method of safeguarding, the foreign exchange transaction funds will need to be segregated from the payment service transaction funds. Once the foreign exchange transaction has taken place, if the PI pays those funds on to a third party on behalf of its client, and this amounts to a payment service, the PI will need to safeguard the currency purchased in the foreign exchange transaction as soon as it receives it. To be clear, in our view in making a payment of currency to its customer in settlement of a foreign exchange transaction the FX firm will be acting as principal in purchasing the other currency from its customer. This does not constitute a payment service. Firms combining payment and non-payment services in this way will need to be clear in their prior information to customers when they are providing regulated payment services (and therefore funds will be safeguarded) and when they are not.

Firms which operate outside the EEA should note that transactions where both the payer and the payee are outside the EEA (for example a transfer between Japan and Hong Kong) are outside the scope of the safeguarding provisions of the PSRs, and as such funds received for these transactions should not be included in segregated funds

There are two ways in which a PI may safeguard relevant funds:

The first method requires the PI to segregate the relevant funds from all other funds it holds. This requirement applies as soon as funds are held by a PI. If relevant funds continue to be held at the end of the business day after the day the PI received them, the PI must:

- deposit the relevant funds in a separate account it holds with an authorised credit institution; or
- invest the relevant funds in secure, liquid assets approved by the FCA and place those assets in a separate account with an authorised custodian.

An authorised credit institution includes UK banks and building societies authorised by the PRA/FCA to accept deposits (including UK branches of third country credit institutions) and EEA firms authorised as credit institutions by their home state competent authorities. Authorised custodians include firms authorised by the FCA to safeguard and administer investments and EEA firms authorised as investment firms under the Markets in Financial Instruments Directive ("**MiFID**") and which hold investments under the standards in Article 13 of MiFID.

The safeguarding account in which the relevant funds or equivalent assets are held must be named in a way that shows it is a safeguarding account (rather than an account used to hold money belonging to the PI). The safeguarding account must not be used to hold any other funds or assets. In the FCA's view, the effect of having to hold a separate account that only the PI may have any interest or right over the relevant funds or assets in that account (except as provided by regulation 19) is that PIs cannot share safeguarding accounts. For example, a corporate group containing several PIs cannot pool its respective relevant funds or assets in a single account. Each PI must therefore have its own safeguarding account. The PSRs do not, however, prevent PIs from holding more than one safeguarding account. If an account with an authorised credit institution is being used, it is important that the account is named in such a way that its purpose is clear, and that the PI has an acknowledgement from the account-holding credit institution or is otherwise able to demonstrate that the bank has no rights (for example, of set off) over funds in that account. In order to ensure it is clear what funds have been segregated and in what way, PIs must keep records of any:

- relevant funds segregated;
- relevant funds placed in a deposit account; and
- assets placed in a custody account

Regulation 19(5)(b) requires that any such assets are approved by the FCA as being secure and liquid. As the safeguarding provisions in the PSRs and EMRs are very similar, for consistency the FCA uses a common approach for the PSRs and the EMRs in identifying suitable assets.

The FCA has approved the assets referred to below as "liquid". On this basis, these assets are both secure and liquid, and PIs can invest in them and place them in a separate account with an authorised custodian in order to comply with the safeguarding requirement, if they are: (a) items that fall into one of the categories set out in Table 1 of point 14 of Annex 1 to Directive 2006/49/EC(a) for which the specific risk capital charge is no higher than 0%; or (b) units in an undertaking for collective investment in transferable securities ("**UCITS**"), which invests solely in the assets mentioned previously.

A PI may request that we approve other assets. We will make our decision on a case by case basis, with the firm being required to demonstrate how the consumer protection objectives of safeguarding will be met by investing in the assets in question. Authorised custodians include firms authorised by the FCA to safeguard and administer investments and EEA firms authorised as investment firms under the MiFID and that hold investments under the standards in Article 13 of MiFID.

The second safeguarding method is to arrange for the relevant funds to be covered by an insurance policy with an authorised insurer, or a guarantee from an authorised insurer or an authorised credit institution. The policy or guarantee will need to cover all relevant funds, not just funds held overnight or longer. It is important that the insurance policy or guarantee specifically covers the areas set out here. The proceeds of the insurance policy or guarantee must be payable in an insolvency event (as defined in regulation 19) into a separate account held by the payment institution. That account must be named in a way that shows it is a safeguarding account (rather than an account used to hold money belonging to the PI). The account must not be used for holding any other funds, and no-one other than the PI may have an interest in or right over the funds in it (except as provided by regulation 19).

Neither the authorised credit institution nor the authorised insurer can be part of the corporate group to which the PI belongs. Where a PI that has chosen to deposit customer funds in a bank account or invest them in secure, liquid assets, is placed in administration or ‘wound up’ these funds shall form part of the firm’s asset pool and the claims of the payment service user will be paid from the asset pool in priority to all other creditors. Regulation 19(11) ensures that, provided the funds have been safeguarded in accordance with one of the methods described above, the users’ funds are protected from the claims of other creditors. In this case the asset pool includes all individual customer funds below £50 that the PI has chosen to safeguard voluntarily.

PIs must maintain organisational arrangements that are sufficient to minimise the risk of the loss or diminution of relevant funds or assets through fraud, misuse, negligence or poor administration. This requirement is in addition to the general requirements on authorised PIs to have effective risk management procedures, adequate internal control mechanisms and to maintain relevant records, and applies to both authorised PIs and small PIs that voluntarily safeguard. A PI’s auditor is required to tell the FCA if it believes that there is or has been, may be or may have been, a breach of regulation 19 of material significance to the FCA, including a breach of the organisational arrangements requirement.

If an insolvency event (listed in regulation 19(15)) occurs in relation to an authorised PI or a small PI that is voluntarily safeguarding then, with one exception, the claims of payment services users will be paid from the relevant funds and assets that have been segregated (the ‘asset pool’) in priority to all other creditors. The exception is that expenses of the insolvency proceeding take priority so far as they are in respect of the costs of distributing the asset pool. No right of set-off or security right can be exercised in respect of the asset pool, except to the extent that it relates to fees and expenses in relation to operating a safeguarding account.

(b) E-Money

The EMRs impose safeguarding requirements to protect customer funds. If a business that has safeguarded funds becomes insolvent, the claims of e-money holders (and payment service users where appropriate) are paid from the asset pool formed from these funds above all other creditors (except for the costs of distributing the asset pool).

All EMIs are required by regulation 20 of the EMRs to safeguard funds received in exchange for e-money that has been issued (i.e., "relevant funds").

A credit union that issues e-money will have a Part 4A permission under FSMA to issue e-money but is required under the EMRs to safeguard funds received in exchange for e-money as if it were an EMI (see regulation 20(5) of the EMRs).

EMIs and credit unions are entitled to provide payment services that are unrelated to the issuance of e-money. Authorised EMIs that provide unrelated payment services are subject to the safeguarding provisions of the PSRs (regulation 19 of the PSRs) as if they were authorised payment institutions. Small EMIs that provide unrelated payment services are in the same position as small payment institutions with respect to safeguarding.

Under the PSRs small payment institutions can choose to comply with safeguarding requirements for funds received for payment services to offer the same protection over customer funds as authorised payment institutions must provide. If a small EMI chooses to safeguard funds received for unrelated payment services it will have to deliver the same level of protection as is expected of an authorised EMI (and authorised payment institution), as described in this chapter. The FCA requires businesses applying to become small EMIs that provide unrelated payment services to tell the FCA if they will safeguard these funds. Those that opt to safeguard funds received for unrelated payment services will have to provide information about their safeguarding arrangements in annual reporting returns to the FCA. Credit unions are subject to regulation 19 of the PSRs on the same basis as small EMIs.

Relevant funds received in the form of payment by a payment instrument only have to be safeguarded when they are credited to the EMI's or credit union's payment account or are otherwise made available to the EMI or credit union, but must be safeguarded by the end of five business days after the date on which the e-money has been issued. This relates to e-money paid for by a payment instrument such as a credit or debit card and not e-money that is paid for by cash, even if the cash payment is received by a person acting on behalf of the EMI or credit union (such as an agent or distributor).

Authorised EMIs must also separately safeguard funds received in exchange for unrelated payment services. Small EMIs and credit unions may choose to safeguard funds received in exchange for unrelated payment services. Funds received in exchange for unrelated payment services and relating to a particular payment transaction only have to be safeguarded if they exceed £50 (in which case the full amount must be safeguarded, not just the amount by which the funds exceed the £50 threshold). EMIs and credit unions may, however, choose to safeguard amounts beneath this threshold, in which case the insolvency protections will apply.

Some EMIs will also receive funds from the public in respect of other services. An example is an EMI with a foreign exchange business. EMIs with such hybrid businesses are only required to safeguard the funds received for e-money. However, sometimes such hybrid businesses will not know the precise proportion of customer funds received for e-money or the amount may be variable. In these circumstances, an EMI may make a reasonable estimate on the basis of relevant historical data of the proportion that is likely to be for e-money and this proportion must be safeguarded. The EMI would, if asked, have to satisfy the FCA that the proportion actually safeguarded was a reasonable estimate. Relevant data might include the proportion generally used as e-money by the customer in question or by similar customers generally.

In the FCA's view, an EMI that is carrying out a foreign exchange transaction independently from its payment services (see Qestion 12 in PERG 15.2) does not have to safeguard funds received for the purpose of the foreign exchange transaction. Once the foreign exchange transaction has taken place, if the EMI pays those funds on to a third party on behalf of its client, and this is a payment service, the currency purchased in the foreign exchange transaction becomes relevant funds and should be safeguarded as soon as it is received if appropriate. EMIs and credit unions combining payment and non-payment services in this way will have to be clear in the information they provide to customers prior to the transaction which parts of the service are regulated (and therefore funds are safeguarded) and which parts are not, to avoid breaching the Consumer Protection from Unfair Trading Regulations 2008.

According to the FCA, it is important that the availability of an asset pool from which to pay the claims of e-money holders or payment service users in priority to other creditors in the event of the insolvency of an EMI is not undermined by the EMI improperly mixing funds, assets or proceeds received or held for different purposes. For example, if an account that an EMI holds with a credit institution is used not only for holding funds received in exchange for e-money but also for funds received for the execution of payment transactions not related to issuing e-money, or funds received for other activities (such as foreign exchange), this is likely to corrupt the segregation. This may result in the protection for e-money holders in regulation 24 not applying. As a further illustration, an authorised EMI may safeguard funds received in exchange for e-money by covering them with an insurance policy or guarantee. However, if the account into which the proceeds of the insurance policy or guarantee are payable is also used for holding funds for other activities, or for holding the proceeds of another insurance policy taken out to safeguard funds received for payment transactions not related to issuing e-money, then this may mean that the proceeds are not considered to be an asset pool subject to the special rules about the priority of creditors in the event of an insolvency.

There are two ways in which an EMI or credit union may safeguard relevant funds:

- The first method requires the EMI/credit union to segregate funds received in exchange for e-money (relevant funds) from any other funds it holds including its working capital and funds received for other business activities for example, foreign exchange transactions. Relevant funds must be held separately from funds received for the execution of payment transactions not related to issuing e-money. This requirement applies as soon as funds are held by the EMI/credit union and includes money received on its behalf by agents or distributors.

- The second safeguarding method is to arrange for the relevant funds to be covered by an insurance policy with an authorised insurer, or a guarantee from an authorised insurer or an authorised credit institution. EMIs/credit unions also safeguarding funds received for payment transactions that are not related to issuing e-money may need a separate policy or guarantee to ensure both sets of funds are adequately covered.

Where an EMI/credit union that has chosen to deposit customer funds in a credit institution account or invest them in secure, low risk and liquid assets, is placed in administration or ‘wound up’, these funds shall form part of the EMI’s/credit union’s asset pool. The claims of the e-money holder/payment service user will be paid from the asset pool above all other creditors. Regulation 24(1) of the EMRs and regulation 19(11) of the PSRs ensure that, provided the funds have been safeguarded in accordance with one of the methods described above, the users’ funds are protected from the claims of other creditors. The claims of the e-money holder/payment service user are not subject to the priority of expenses of an insolvency proceeding except in respect of the costs of distributing the asset pool. The asset pool will include all individual customer funds for payment transactions unrelated to e-money issuance where a small EMI or credit union has chosen to safeguard such individual transactions (which they are not obliged to do). The asset pool will also include all individual customer funds for unrelated payment transactions at or below £50 that an authorised EMI has chosen to safeguard voluntarily, as again the authorised EMI is not obliged to safeguard unrelated payment transactions below £50.

EMIs/credit unions must maintain organisational arrangements that are sufficient to minimise the risk of the loss or reduction of relevant funds or assets through fraud, misuse, negligence or poor administration (regulation 24(3) of the EMRs and regulation 19(14) of the PSRs). This requirement is in addition to the general requirements on EMIs and credit unions to have effective risk management procedures, adequate internal control mechanisms and to maintain relevant records. It also applies to small EMIs and credit unions that voluntarily safeguard funds received for unrelated payment services.

An EMI’s or credit union’s auditor is required to tell the FCA if it has become aware in its capacity as an auditor that, in its opinion, there is or has been, may be or may have been, a breach of any requirements imposed by or under the EMRs that is of material significance to the FCA (regulation 25(4) of the EMRs). This may be in relation to either or both the issuing of e-money and the provision of unrelated payment services, and includes a breach of the safeguarding requirement and the organisational arrangements requirement.

If an insolvency event (as listed in regulation 24 of the EMRs) occurs in relation to an EMI or credit union that is safeguarding, then (with one exception) the claims of e-money holders will be paid from the relevant funds and assets that have been segregated (the ‘asset pool’ as defined in regulation 24 of the EMRs) above all other creditors. The exception is that expenses of the insolvency proceeding take priority so far as they are in respect of the costs of distributing the asset pool. No right of set-off or security right can be exercised in respect of the asset pool, except to the extent that it relates to the fees and expenses of operating a safeguarding account.

We are not aware of any authorised EMIs or PIs which have become insolvent in the UK.

8. Information Requirements

(a) Payment Services

Parts 5 and 6 of the PSRs set out obligations on payment service providers relating to the conduct of business in providing payment services. These are typically referred to as ‘conduct of business requirements’.

They fall into two main categories:

- information to be provided to the customer before and after execution of a payment transaction; and
- the rights and obligations of both payment service provider and customer in relation to payment transactions.

The requirements apply to all payment service providers except credit unions, municipal banks and the National Savings Bank. Broadly, the requirements apply to all payment transactions where the payment service providers of both the payer and the payee are located in the EEA, and where the payment transactions are in euro, or in the currency of a member state that has not adopted the euro. The exception is regulation 73 of the PSRs which applies to all transactions, including one leg transactions, i.e. those where the payment service provider of either the payer or the payee is located outside the EEA.

The information that payment service providers are required by the PSRs to provide to customers is separated into two scenarios as follows:

- **Transactions under framework contracts –** that is, a contract governing the future execution of individual and successive payment transaction. This is where there is an ongoing relationship, and there is an agreement between the payment service provider and the customer covering the making of payments. An example of this would be parts of a bank’s current account terms and conditions. It is important to understand that payment transactions falling under the scope of the PSRs are also made to and from accounts other than payment accounts, and that where this is the case, the framework contract provisions will also apply to the payment service provider’s agreement with its customers. No account to or from which payment transactions falling within the scope of the PSRs are made can therefore correctly be said to be ‘out of scope of the PSRs’, and payment service providers must ensure that they take this into consideration in their arrangements for such accounts. However, there are some provisions that we believe will only apply to payment accounts and these are explained later in this chapter.
- **Single payment transactions –** this is typically where there is no ongoing relationship between the customer and the payment service provider – the transaction is a ‘one-off’ and the contract between the payments service provider and the customer relates solely to the particular transaction in question. A single payment transaction may also occur if there is a framework contract that does not include the particular payment service involved.

For both scenarios, the PSRs set out the information to be provided before the contract is entered into, at the time the payment order is made, and after execution of the transaction.

For some customers, as detailed below, different arrangements may be made by agreement. It is important to note that the PSRs provide that the agreement may be that ‘any or all of the provisions do not apply’. In the FCA's view, for the customer to ‘agree’ it must be made clear to them which provisions are being disapplied. Payment service providers are allowed to agree different terms with certain classes of business customers. This is known as the ‘corporate opt-out’. However, this is only where the customer is not:

- a consumer;
- a micro-enterprise[3]; or
- a charity with an annual income of less than £1 million

Specific information required to be provided by the PSRs before the contract is made is contained in Schedule 4, covering:

- Details about the payment service provider;
- Details of the payment service(s) to be provided;
- Charges and interest;
- Transmission of information;
- Information about safeguards and corrective measures;
- Information about the length of the contract, variation of terms and termination;
- Information on applicable law and disputes.

While we have not provided detailed summaries of each of the conduct of business requirements in the PSRs. However, we summarise some of the key provisions below:

- *Regulation 59 - Notification of unauthorised or incorrectly executed payment transaction* - If a customer becomes aware of an unauthorised or incorrectly executed payment transaction, he must notify the payment service provider concerned without undue delay and no later than 13 months after the date of the transaction, or else he will not be entitled to redress under the PSRs. However, it should be noted that payment service providers have the ability to grant more favourable terms to their customers, and therefore to offer a longer period (for example, the UK Direct Debit Guarantee Scheme would not be prevented from continuing to offer a longer period for refunds). The time limit above will not apply where the payment service provider has failed to comply with any of the information requirements imposed by the PSRs in respect of the transaction concerned. This provision will not apply if the contract under which the payment service is provided is a regulated agreement under the Consumer Credit Act 1974 (as amended) ("CCA") and instead other provisions will apply. These provisions generally replicate or are more advantageous to the customer than, the PSR provisions. This provision cannot be opted out of.
- *Regulation 61 - Payment service provider’s liability for unauthorised transactions* - If a payment transaction was not properly authorised by the customer, the payment service provider concerned must immediately refund the amount of the transaction to the payer and, if applicable, restore the relevant payment account to the state it would have been in had the transaction not been made. A transaction should be treated as unauthorised unless the payment service provider has the consent of the customer as set out in regulation 55 of the PSRs. Where consent has been withdrawn by the customer for either a specific payment transaction or a series of payment transactions, including the payment transaction in question, it should be treated as unauthorised. There is a balance to be struck between a customer’s right to an immediate refund for an unauthorised payment transaction, and the need to determine whether the payment transaction was properly authorised, or whether the customer

[3] A "micro-enterprise" is an enterprise that employs fewer than ten people and has a turnover or annual balance sheet that does not exceed €2m.

has failed in their own obligations with regard to the payment instrument used, so that the claim is invalid. The FCA expects payment service providers to take a reasonable approach to this. In the FCA's view it would usually be reasonable to investigate a claim before making a refund if there is prima facie evidence to suggest that either the customer has acted fraudulently or that he has deliberately or grossly negligently failed to comply with his obligations in relation to the payment instrument. Otherwise, the FCA would generally expect the payment service provider to make the refund and other correcting actions immediately. The FCA considers that the reference in regulation 61 of the PSRs to 'immediately' refunding the amount of an unauthorised payment transaction means that the payment service provider must refund the amount as quickly as possible. In the FCA's view, any refund made later than close of business on the day the claim was made could not be regarded as immediate. The only exception to this would be if the claim was received out of hours or at the very end of the business day. In such circumstances it may be acceptable to make the refund at the beginning of the following business day. If a claim is to be investigated before making the refund, the decision to do so must generally be made on the business day the claim is made, and must be on the basis of prima facie evidence to support possible customer liability. The reasons for such a decision should be recorded in case of any challenge. Where an investigation is justified, it needs to be carried out as quickly as possible in light of the circumstances. The FCA generally expects this to mean days rather than weeks; in no circumstances should the investigation be used to discourage the customer from pursuing the claim. Clearly, if such an investigation is carried out and the customer is not found to be at fault, an immediate refund must be made, and back valued so that the customer does not suffer any loss. There is nothing to prevent the payment service provider from investigating a claim after having made the refund and, if the results of such investigation enable it to prove either that the customer did authorise the transaction or was otherwise liable, reversing the refund. Where this occurs, the FCA expects the firm to give reasonable notice of the reversal to the customer. What is 'reasonable' will depend on the particular circumstances of the case. For agreements regulated by the CCA other provisions will apply. For low value payment instruments, if the nature of the instrument is such that it is not possible for the payment service provider to prove that it was authorised (for example, if it was used anonymously) this provision will not apply. This provision cannot be opted out of.

- *Regulation 62 - Payer's liability for unauthorised payment transactions* - The payer will be liable for losses up to a maximum of £50 resulting from unauthorised transactions arising from the use of a lost or stolen payment instrument, or from the misappropriation of the payment instrument where they have failed to keep its personalised security features safe. It should be noted that the £50 liability limit is applicable to each instance of loss, theft or misappropriation, and not to each transaction. In the FCA's view, in this context, personalised security features means features such as the password or PIN relating to the payment instrument. It does not include information that is readily readable from the payment instrument itself (for example, a card number or security code printed anywhere on a card), as this information will be readily available to any merchant or business where the card has been used. If the payment service provider can show that the payer has acted fraudulently, or has intentionally, or with gross negligence, not complied with their obligations regarding the security of the payment instrument, the payer will be liable for all losses. To avoid doubt, it is not sufficient for the payment service provider to assert that the customer 'must have' divulged the personalised security features of the payment instrument, and to effectively require the customer to prove that he did not. The burden of proof lies with the payment service provider and if a claim that a transaction is unauthorised is rejected, the rejection must be supported by sufficient evidence to prove that the customer is guilty of fraud, gross negligence or intentional breach and the reason for the rejection must be explained to the customer. Except where the payer has acted fraudulently, the payer is not liable for any losses: (a) arising after they notified the payment service provider of the loss, theft or misappropriation (this will not apply for low value payment instruments if the nature of the instrument means that it is not possible for the payment service provider to prove that the transaction was authorised – because, for example it is used anonymously - or to stop the payment instrument from being used; (b) if the payment service provider has failed to provide the means for the payer to make the notification (subject to the force majeure provisions of regulation 79 of the PSRs); or (c) where the payment instrument has been used in connection with a distance contract other than an excepted contract (as defined in the Consumer Protection (Distance Selling) Regulations 2000). The corporate opt-out applies to this provision (see above).

- *Regulation 70 - Payment transactions to a payment account – time limits for payment transactions* - The default rule is that payments have to be credited to the payee's payment service provider's account (that is the payee's PSP's account with its own bank or settlement service provider) by close of business on the business day following the day when the payment order was received (or was deemed to have been received). An extra day may be added to the above period when the payment order is initiated in paper, rather than electronic form. For payment transactions in the currency of an EEA State where (a) both the payer and the payee are within the EEA; and (b) the payment transaction is not a UK national sterling transaction; and (c) the payment transaction is not in euro, (d) the maximum period that may be agreed between the payer's payment service provider and its customer is the end of the fourth business day following the day on which the payment order was received. The payee's payment service provider must value date and make available the credit to the payee's account following receipt of the funds in its own account in accordance with regulation 73 of the PSRs. Therefore, as soon as the funds are received in the payee's payment service provider's account, it must make sure that the payee can get access to the funds and credit value date them no later than the business day on which the payment service provider's account was credited. In practice this means that payment service providers' systems must identify the funds immediately they are received in their own account with their settlement provider and credit them to the payee's account immediately. If the funds are received on a non-business day, the above requirements will apply at the start of the next business day. Payment transactions where both the payer's and the payee's accounts are with the same payment service provider are within the scope of the PSRs, and as such the execution time provisions will apply. This includes transactions where the payer and the payee are the same person. Where an external clearing system is used to execute the transaction, the FCA's view is that the funds will be 'credited to that payment service provider's account' (regulation 73(2)) when that clearing system settles, in the same way as payments received from another payment service provider through that clearing system. This provision cannot be opted out of.

- *Regulation 71 - Absence of payee's payment account with the payment service provider* **-** Where the payee does not hold a payment account with the payment service provider (for example, in money remittance services) the payment service provider to which the payment has been sent must make the funds available immediately after they have been credited to its account. This provision should not be seen as requiring banks which receive funds addressed to a payee for whom they do not hold an account to hold such funds pending collection by the payee.

- *Regulation 73 - Value date and availability of funds* **- T**he value date of a credit to a payment account can be no later than the business day on which the payment transaction was credited to the payee's payment service provider's account. This is the business day on which the payee's payment service provider is deemed to have received the funds. The funds must also be at the payee's disposal immediately after they have been credited to the payee's payment service provider's account. Where the payee's account is not a 'payment account' and the payee's payment service provider is a credit institution/bank, the rule in BCOBS 5.1.13 will apply, so that the transaction must be value date don the business day received, but availability must be within a reasonable period.

(b) E-Money

Part 5 of the EMRs sets out obligations that apply to the conduct of e-money business where it is carried out from an establishment maintained by an electronic money issuer or its agent or distributor in the UK. These are typically referred to as 'conduct of business requirements'. They relate to issuing and redeeming e-money and the prohibition on the payment of interest or other benefits linked to the length of time that e-money is held and are applicable to all electronic money issuers.

Regulation 39 of the EMRs requires electronic money issuers to issue e-money at par value (the e-money issued must be for the same amount as the funds received) when they receive the funds and without delay. It is important to recognise that if an agent of an electronic money issuer receives funds, the funds are considered to have been received by the issuer itself. It is not, therefore, acceptable for an electronic money issuer to delay in enabling the customer to begin spending the e-money because the issuer is waiting to receive funds from its agent or distributor.

Under the EMRs, e-money holders have the right to redeem the monetary value of their e-money (that is the payment from the electronic money issuer to the e-money holder of an amount equivalent to the remaining balance) at any time and at par value (regulation 39 of the EMRs). This means that, in the FCA's view, it is not acceptable to have a term in a contract with an e-money holder under which the e-money holder's right to redeem the remaining balance ceases to apply after a specified period of validity (although the contract can still provide for the e-money holder's right to use the e-money for the purpose of making payment transactions to cease after a specified period). This is qualified by regulation 43 of the EMRs which allows electronic money issuers to refuse a redemption request when the request is made more than six years after the date of termination in the contract. The contract between the electronic money issuer and the e-money holder must, clearly and prominently, set out the conditions of redemption (or part thereof), including any fees that may be payable. These conditions must be advised to e-money holders before they are bound by the contract.

The PSRs set out conduct of business requirements for all payment service providers, including electronic money issuers. In this context, this means requirements for information to be provided to payment service users, and specific rules on the respective rights and obligations of payment service users and providers. Electronic money issuers should consider these requirements and comply with them to the extent that they relate to their business of issuing e-money and the payment services that they provide.

9. Complaints

EMRs

Complaint handling covers three distinct areas (a) how electronic money issuers handle the complaints they receive from customers; (b) the role of the FOS in dealing with complaints where customers are not satisfied with the company's response; and (c) the FCA's role in handling complaints from customers and other interested parties about electronic money issuers' alleged breaches of the EMRs and about the FCA.

The Second Electronic Money Directive requires there to be an adequate and effective out-of-court complaint and redress procedure to settle disputes between electronic money issuers and e-money holders or payment service users. FSMA is amended to allow the ombudsman service to operate an out-of-court complaint and redress process for electronic money issuers. This means that the rules relating to complaints handling are not in the EMRs but in the Dispute Resolution: Complaints sourcebook ("**DISP**") in the FCA Handbook.

All electronic money issuers are subject to the complaints handling rules even if they are not required to be authorised or registered by the FCA.

The rules about how electronic money issuers should handle complaints are set out in Chapter 1 of DISP. The rules cover a range of issues, including aiding consumer awareness, establishing internal complaint-handling procedures, timeliness, the requirement for a final response letter, rules on referral of complaints to others and a requirement to cooperate with the ombudsman service.

All electronic money issuers except those with Part 4A permission under FSMA to issue e-money are exempt from the requirements in these rules to record complaints, report complaint statistics to the FCA, or publish their complaints data. However, it is in their interests to retain records of complaints so these can be used to help the ombudsman service if necessary. This does not affect any requirements to record or report complaints if they are authorised by the FCA to undertake any other regulated activity. Firms authorised under FSMA to issue e-money (credit institutions, municipal banks and credit unions) are not exempt from the complaints record rule, the complaints reporting rules or the complaints data publication rules.

PSRs

Complaint handling covers three distinct areas (a) how payment service providers handle the complaints they receive from customers (b) the role of the FOS in dealing with complaints where customers are not satisfied with the company's response; (c) the FCA's role in handling complaints from customers and other interested parties about alleged breaches of the PSRs.

Payment service providers are subject to our rules about how they handle complaints. These rules are set out in Chapter 1 of DISP (see comments above). For firms such as banks (entities with permission to accepts deposits), who fall under the FOS's jurisdiction for activities other than payment services, there is no difference in the arrangements except in respect of the consumer awareness rules. Firms that are only regulated by the FCA in relation to payment services are not required to record complaints, report complaint statistics to the FCA, or publish their complaints data. However, it is in firms' interests to retain records of complaints so these can be used to help the FOS if necessary. Firms that are regulated by the FCA in relation to other activities must record and report on all complaints, including payment service complaints and publish a summary of their complaints data if they receive 500 or more complaints in any half-year reporting period.

The PSRs require firms to provide information about the out-of-court complaint and redress procedures for the payment service user and the methods for having access to them (paragraph 7(b) of Schedule 4). This means informing payment service users about the firm's own complaints mechanism and the availability of the FOS. This information can be provided using the summary details required under DISP 1.2. For single payment transactions, this information must be made available 'in good time before the payment service user is bound by the single payment service contract'. For framework contracts, this information must be provided 'in good time before the payment service user is bound by the framework contract'. In both cases, where the contract is concluded using distance means, the information can be provided immediately after conclusion of the contract if the method used to conclude the contract does not enable earlier provision.

10. Distance Contracts

If the contract for the provision of payment services is a distance contract, additional information obligations apply. A contract entered into by the payment service provider is considered a distance contract if the other party to the contract is a consumer and the contract is concluded without the simultaneous physical presence of the payment service provider and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded. Means of distance communication include phone calls and text messages, websites and post. Examples of when distance contracts may be entered into include the online application for a charge card.

The Distance Marketing Directive ("**DMD**") provides protection for consumers whenever they enter into a financial services contract by distance means, including for payment services. Both the PSRs and the DMD apply to contracts for payment services.

When a distance contract is entered into with a customer, the DMD requires a firm to provide the customer with information on a number of matters. This includes information about the firm; the service being provided (including notice of any special risks involved with the investments in question); the contract with the firm (for example, when and how any contract will come into existence and its governing law); the price payable; any right to cancel the contract; and the redress mechanisms available to the customer.

During the term of the contract the customer may request, at any time, the provision of the terms of the contract (including all applicable standard terms, pricing and any other agreed provision) in printed form (e.g. by regular mail or fax, e-mail is likely to be not sufficient). This right of the customer exists even if the customer has already received a hardcopy of the aforementioned information before entering into the contract.

11. Data Protection Provisions

The Data Protection Act 1998 ("**DPA**") implemented the EU Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

The DPA applies to the "processing" of "personal data", both of which terms are very widely defined. This means that practically any business operating in the UK which holds information about individuals (whether employees, customers or anyone else) is affected by the DPA. Breaches of data protection laws can result in criminal as well as civil liability.

All of the obligations under the DPA fall on the data controller. This is defined as the person who (either alone, jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is, or is to be, processed.

The DPA applies only to personal data. Data is defined as information which is being processed by means of equipment that operates automatically in response to instructions given for that purpose, or is recorded with the intention that it should be processed by means of such equipment. The DPA therefore applies to automated data, such as that stored on a computer. It also extends to certain manual records.

Personal data is data relating to living individuals who can be identified from that data, or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller. Personal data includes, for example:

- Names.
- Addresses.
- Telephone numbers.
- Job titles.
- Dates of birth.

The DPA applies to many different types of data and a wide range of processing activities, and imposes a range of obligations on data controllers to ensure that data is processed properly. Schedule 1 of the DPA sets out a number of data protection principles, which require that:

- Data must be processed fairly and lawfully

- Data must be obtained only for specified lawful purposes and not further processed in a manner which is incompatible with those purposes.
- Data must be adequate, relevant and not excessive in relation to the purposes for which it is processed. In practice, this means that data controllers must keep existing data under review.
- Data must be accurate and, where necessary, kept up to date. Generally, controllers are required to update all databases unless they constitute a static archive.
- Data must not be kept for longer than is necessary
- Data must be processed in accordance with the rights of data subjects under the DPA
- Appropriate technical and organisational security measures must be taken to prevent unauthorised or unlawful processing, accidental loss of or destruction or damage to personal data
- Personal data must not be transferred outside the EEA unless the destination country ensures an adequate level of protection for the rights of the data subject in relation to the processing of personal data

The Information Commissioner's Office produces a Guide to Data Protection. The guide is for those who have day-to-day responsibility for data protection. It explains the purpose and effect of each principle, gives practical examples and answers frequently asked questions. It also contains specialist topics including CCTV, employment and data sharing. The guidance is not binding on firms.

12. General Laws applicable to Payment/E-Money Services

As well as the PSR and EMR, payment and e-money services must also comply with relevant general laws in the UK. Payment service and e-money providers must, in addition to the PSRs and EMRs, abide by UK consumer protection laws, data protection laws, FCA rules and, in certain circumstances, consumer credit laws. In some scenarios, firms may be able to comply with certain rules which will allow them to deviate from some of the general laws. However, on the whole, firms must comply with both the PSR or EMR and the general laws described below.

All payment service and e-money providers must comply with UK consumer protection law. Currently, UK consumer protection law is found in multiple acts such as the Sale of Goods Act, the Sale of Goods and Services Act and the Unfair Contracts Term Act. A detailed summary of all applicable consumer protection laws can be found in the UK Research Report 2 and 3. In 2015, the UK Parliament is debating a Consumer Protection Bill that will condense many of the laws into one Act.

All payment service and e-money providers must also comply with UK data protection laws, summarised under heading 9 above.

In addition, if a payment service or e-money provider is offering credit, loans or debt services, they must follow laws regarding consumer credit. These laws can be found in the Consumer Credit Act 1974, various statutory instruments and in the FCA handbook ("**CONC**"). Firms wishing to carry out these activities must also be authorised by the FCA to offer consumer credit.

13. Voluntary/Self-Disciplinary Rules of Banking/Financial Associations in the UK

(a) Payment Services

There is guidance in PERG[4]. The purpose of PERG is to give guidance about the circumstances in which authorisation under FSMA is required, and guidance on the exclusions which are available.

[4] http://fshandbook.info/FS/html/handbook/PERG

The relevant section in PERG for payment service providers is PERG 15, which gives guidance on the scope of the PSRs. PERG 15 acknowledges that the PSD regulations create a separate authorisation and registration regime which differs from the authorisation requirements under the FSMA. PERG 15 is therefore it is aimed at helping businesses consider whether they need to be separately authorised or registered for the purposes of providing payment services in the UK. As this is guidance, it is not binding on firms but it does explain how the FCA interpret the provisions in the PSRs.

The FCA have also issued an 'Approach to Payment Services' document[5] (dated June 2013). This document describes the FCA's approach to implementing the PSRs. It gives payment service providers links to all the information they need to have a comprehensive picture of the payment services regime. It also provides guidance to give payment service providers a practical understanding of the requirements, the FCA's regulatory approach and how businesses will experience regulatory supervision. This document is illustrative guidance and, as such, is not binding on payment service providers.

The European Commission have guidance relating to the PSD, the directive which underlies the PSRs, in the form on questions and answers on their websites. These Q&As allow for firms to submit questions they have regarding the PSD and the Commission will then answer them with their interpretation of the provision in question. Although these are not binding, they provide a source of guidance for firms wanting clarity on particular provisions of the PSD.

(b) E-Money

There is also guidance in PERG for e-money institutions. The relevant section in PERG for e-money providers is PERG 3A, which gives guidance on the scope of the EMRs. PERG 3A is intended to help these persons providing e-money services to consider whether they need to be authorised or registered for the purposes of e-money issuance in the UK. Again, as this is only guidance it is not binding on firms, but explains the FCA's interpretation of the EMRs.

The FCA have also issued an 'Approach to E-Money' document[6] (dated June 2013). This document describes the FCA's approach to interpreting and applying the EMRs . It gives firms links to the information they need for a comprehensive picture of the regulatory regime , as it is primarily aimed at businesses that are currently issuing or considering issuing e-money. It also provides guidance to give e-money issuers a practical understanding of the requirements, the FCA's regulatory approach and how businesses experience regulatory supervision depending on the type of e-money issuer. This document is illustrative guidance and, as such, is not binding on payment service providers.

(c) Money Laundering

The Joint Money Laundering Steering Group ("**JMLSG**") is made up of the leading UK Trade Associations in the Financial Services Industry. The JMLSG produces money laundering guidance for the financial sector in conjunction with the Bank of England. The guidance sets out what is expected of firms and their staff in relation to the prevention of money laundering and terrorist financing and allows them some discretion as to how they apply the requirements of the UK anti-money laundering regime in the particular circumstances of the firm, and its products, services, transactions and customers. Although it is guidance, the UK money laundering regulations provide that a court must take account of such industry guidance in determining whether a person or institution within the regulated sector has complied with any of the requirements of the regulations.

14. Banking Secrecy

The UK does not have bank secrecy laws like other jurisdictions. It is therefore not a specific criminal offence to breach obligations of confidence arising in a banking relationship. However, the UK does

[5] http://www.fca.org.uk/static/documents/payment-services-approach.pdf
[6] http://www.fca.org.uk/static/documents/emoney-approach.pdf

have laws imposing obligations on confidentiality . In *Tournier v National Provincial and Union Bank of England*, the court established that it is an implied term of the contract between a banker and his customer that the banker will not divulge to third persons, without the consent of the customer express or implied, either the state of the customer's account, or any of his transactions with the bank, or any information relating to the customer acquired through the keeping of his account, certain exemptions exist to this duty including where the banker is compelled to do so by order of a Court, or the circumstances give rise to a public duty of disclosure, or the protection of the banker's own interests requires it. The Tournier principle applies to banker/client relations (i.e. in a deposit taking context) and not more broadly. In other type of banking style relationship the general law of confidence may impose such obligation or alternatively it might be imposed contractually.

This is not relevant to PIs and EMIs but would be relevant to a bank (see comments below in respect to UK Banking Regulations).

15. Regulations relating to the prevention of Money Laundering

All PIs and EMIs must comply with legal requirements to deter and detect financial crime, which includes money laundering and terrorist financing. Relevant legislation includes the financial crime provisions in the PSRs, section 21A of the Terrorism Act 2000, the Proceeds of Crime Act 2002, the Money Laundering Regulations 2007, the EC Wire Transfer Regulation and Schedule 7 to the Counter-Terrorism Act 2008. PIs and EMIs are also subject to the various pieces of legislation that implement the UK's financial sanctions regime, which acts to freeze the assets of certain individuals and entities designated by the government.

The FCA expect PIs and EMIs to show risk-sensitive anti-money laundering ("**AML**") policies, procedures and internal controls related to:

- customer due diligence checks;
- the ongoing monitoring of business relationships;
- the reporting of suspicions, both within the firm and to the National Crime Agency;
- assessment of money laundering risks and the application of enhanced measures in higher
- risk situations
- record keeping;
- monitoring compliance with procedures;
- internal communication of policies and procedures; and
- staff awareness and training on money laundering matters.

(a) Customer Due Diligence

The Regulations require businesses to carry out certain customer due diligence on all customers for whom they are undertaking work in the regulated sector. Failure to introduce and maintain these systems and procedures is an offence punishable by imprisonment and/or a fine, even if no money laundering takes place. The obligation in the UK is that the verification of the identity of the client and, where applicable, the beneficial owner as part of the due diligence process, must take place before the establishment of a business relationship or the carrying out of an occasional transaction. The Regulations, in addition, require a business to have a system of ongoing monitoring to ensure that customer due diligence information is kept up-to-date.

The Regulations also provide that for certain types of clients assessed to be a lower risk for money laundering purposes, a simplified due diligence process can be applied. Conversely certain categories of clients are considered higher risk, necessitating enhanced due diligence and ongoing monitoring.

For the purposes of the Money Laundering Regulations 2007, customer due diligence procedures mean:

- identify the customer, and verify his identity on the basis of documents, data or information obtained from a reliable and independent source;
- identify the beneficial owner, where relevant, and verify his identity and taking adequate measures on a risk sensitive basis to verify that person's identity so that the relevant person is satisfied that he knows who the beneficial owner is, including in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement; and
- obtaining information on the purpose and intended nature of the business relationship.

Firms will also have to ensure they have:

- enhanced monitor ongoing business relationships;
- approval from senior management of transactions if necessary;
- established the source of wealth of a customer

(b) Simplified Due Diligence

The Regulations provide that for certain types of customers assessed to be lower risk for money laundering purposes, a simplified due diligence process can be applied. Very broadly, simplified due diligence applies to:

- credit or financial institutions subject to the requirements of the Money Laundering Directive or equivalent AML legislation;
- companies whose securities are listed on a regulated market subject to specified disclosure obligations;
- UK public authorities; and
- UK pension schemes.

If a customer falls within a simplified due diligence category, a firm need only obtain evidence that the customer and the customer transaction (or product related to such transaction) is eligible for simplified due diligence. In practice, this means that so long as the firm does not have a suspicion of money laundering, they do not have to verify the client's identity or, where relevant, that of a beneficial owner, nor must they obtain information on the intended nature and purpose of the business relationship. The firm will still, however have to conduct ongoing monitoring of the business relationship.

(c) Enhanced due diligence

Enhanced due diligence requires additional documents, data or information to establish identity and source of funds for:

- non face-to-face clients;
- politically exposed persons ("**PEPs**");

- clients or beneficial owners of clients with high-risk country or
- clients whose matters involve any other high-risk factors.

(d) Timing of verification and when it must be carried out

Client due diligence measures must be carried out where firms:

- Establish a business relationship.
- Carry out an occasional transaction. An occasional transaction means a transaction (carried out other than as party of a business relationship) amounting to €15,000 or more whether the transaction is carried out in a single operation or several operations which appear to be linked).
- Where money laundering or terrorist financing is suspected;
- Have doubts about the veracity or adequacy of documents, data or information previously obtained for the purposes of identification or verification.

(e) Recording keeping procedures

Documents relating to the identify of customers must be retained for a minimum period of 5 years from the date that the transaction with the customer ceases. All other records obtained as part of the identification procedure will be retained for the same period (for example financial statements, passports, etc.).

(f) Third Party Reliance

Regulation 17 of the AML Regulations permits firms to rely on due diligence carried out by, broadly, other firms who are authorised credit or financial institutions. Reliance does not, however, absolve firms from the need to ensure that they comply with their own obligations under the Regulations. In this connection, firms need to ensure that the level of customer due diligence carried out by the other firm on which they are relying is consistent with the risk assessment on the client that they have performed. For example, if a firm categorises a client as higher risk, then the firm must ensure that the firm on which it is relying has performed enhanced due diligence to the correct standard.

(g) Staff

Firms need to ensure that relevant and appropriately tailored training is provided to staff in key roles. Firms also need to put in place internal procedures to assess and manage money laundering risks, including the appointment of an AML officer. The AML officer has the responsibility of developing and updating a firm's money laundering policies, operating procedures and monitoring systems. The officer must also report to management and is the contact person for employees wishing to report suspicious transactions.

(h) Terrorism Financing

The Terrorism Act 2000 dictates the requirement to report suspicions of offences relating to terrorist financing. The principal offences are:

- involvement in fundraising: this offence is committed if a firm has knowledge or reasonable cause to suspect that the money or other property raised may be used for terrorist purposes;
- use or possession of money or other property for terrorist purposes: this offence can be committed when a firm have reasonable cause to suspect that money or property may be used for terrorist purposes.

- becoming involved in an arrangement which makes money or other property available to another if the firm knows, or has reasonable cause to suspect, that it may be used for terrorist purposes.
- entering or becoming concerned in an arrangement which facilitates the retention or control by, or on behalf of, another of terrorist property.

It is a defence if the firm did not know, and had no reasonable cause to suspect, that the arrangement was related to terrorist property.

16. Payment Systems

The Payment Systems Regulator ("**PSR**") is a subsidiary of the FCA but has its own statutory objectives and governance, including a Managing Director and Board. The PSR was incorporated in April 2014 and will become fully operational in April 2015.

Payment systems form a vital part of the UK's financial system. They underpin the services that enable funds to be transferred between people and institutions – from large transfers between firms to a contactless payment for your morning coffee. Last year these payment systems processed some 21 billion transactions, worth more than £75 trillion. The PSR has three statutory objectives. These are:

- to promote effective competition in the markets for payment systems and for services provided by those systems, including between operators, payment service providers and also infrastructure providers, in the interests of service−users;
- to promote the development of and innovation in payment systems, in particular the infrastructure used to operate payment systems, in the interests of service−users; and
- to ensure that payment systems are operated and developed in a way that considers and promotes the interests of service−users.

The PSR will work with the FCA, the PRA, the Competition and Markets Authority ("**CMA**"), and other regulators. The FCA oversees market integrity, competition and conduct across the wider financial services industry.

HM Treasury will designate the systems that the PSR will regulate. These will be the largest and most important payment systems which, if they were to fail or to be disrupted, would cause serious consequences for their users. The Treasury issued its consultation "Designation of payment systems for regulation by the Payment Systems Regulator" on 14 October 2014. It has proposed designating the main interbank payment systems, namely Bacs, CHAPS, Faster Payments Service (FPS), LINK, Cheque and Credit Clearing (C&CC) and Northern Ireland Cheque Clearing (NICC) and the two largest card payment systems in the UK, MasterCard and Visa.

For each designated system, all the participants in that payment system will fall under the PSR's remit. Participants in a payment system include the operator that manages or operates that system, the PSPs using that system, and the infrastructure providers to the payment system.

BANKING REGULATIONS AND OTHER - UNITED KINGDOM

1. Overview of the UK banking industry

Following the global financial crisis, the UK has had a review of its system of financial regulation. As a result, the Financial Services Act 2012 came into law, which substantially amended the Financial Services and Markets Act ("**FSMA**"). The new act split the FSA into the Financial Conduct Authority ("**FCA**") and the Prudential Regulation Authority ("**the PRA**").

The UK has a universal banking system, which enables all banks to be licenced to provide a full spectrum of banking business, financial services and payment services.

Please see the following link for a list of authorised banks in the UK: http://www.bankofengland.co.uk/pra/Pages/authorisations/banksbuildingsocietieslist.aspx

2. Definition of a Bank - Regulated Activities

Under UK law there is no concept of a 'banking license', instead in the UK there is an activity based regime. This is essence means that a person must obtain permission for each 'regulated activitiy' it carrys out. UK law considers a bank to be an institution which carries on the regulated activity of "accepting deposits".

This is defined by reference to FSMA and the Financial Services and Markets Act 2000 (Regulated Activities) Order 2001 (the "**RAO**"). All "regulated activities" are set out in the RAO.

Under UK law, the 'general prohibition' in FSMA 2000, s 19 provides that no person may lawfully carry on a 'regulated activity' by way of business in the UK unless he is an authorised person or an exempt person.

The core regulated activity connected with banking business is 'accepting deposits' also known as 'deposit taking', although many banking businesses will in addition have permission for other regulated activities, such as investment business, regulated mortgage business and insurance mediation. Likewise, if a person does not 'accept deposits' but nevertheless carries on other regulated activities it wll need to have permission for each of the regulated activities it undertakes.

RAO, Art 5(1) provides that:

(i) Accepting deposits is a . . . [regulated] activity if–

- money received by way of deposit is lent to others; or
- any other activity of the person accepting the deposit is financed wholly, or to a material extent, out of the capital of or interest on money received by way of deposit.'

The term deposit is defined in the RAO, in Arts 5(2) and (3):

(ii) In paragraph (i), "deposit" means a sum of money, other than one excluded by any of articles 6 to 9 A, paid on terms

- under which it will be repaid, with or without interest or premium, and either on demand or at a time or in circumstances agreed by or on behalf of the person making the payment and the person receiving it; and
- which are not referable to the provision of property (other than currency) or services or the giving of security.

(iii) For the purposes of paragraph (ii), money is paid on terms which are referable to the provision of property or services or the giving of security if, and only if–

- it is paid by way of advance or part payment under a contract for the sale, hire or other provision of property or services, and is repayable only in the event that the property or services is or are not in fact sold, hired or otherwise provided;
- it is paid by way of security for the performance of a contract or by way of security in respect of loss which may result from the non-performance of a contract; or
- without prejudice to sub-paragraph (ii), it is paid by way of security for the delivery up or return of any property, whether in a particular state of repair or otherwise.'

The RAO defines each regulated and also includes a range of exclusions. In the case of the regulated activity of accepting deposits, the exclusions cover both (a) specific types of person - for example, under the RAO, art 6(a)(i), a sum of money is not a 'deposit' if it is paid by any of the Bank of England, the central bank of an EEA State other than the United Kingdom, or the European Central Bank; and (b) payments received for specific purposes for example, a sum is not a deposit if it is received as consideration for the issue of certain kinds of debt securities (RAO, art 9); if it is received in exchange for electronic money (RAO, art 9A); or if it is received by an authorised payment institution (RAO, art 9AB).

We summarise in high level below the "regulated activities" (in addition to accepting deposits) which trigger a licensing requirement if carried on in the UK by way of business:

- issuing e-money;
- effecting or carrying out contracts of insurance as principal;
- dealing in investments (as principal or agent);
- arranging deals in investments;
- arranging home finance activities;
- operating a multilateral trading facility;
- managing investments;
- assisting in the administration and performance of a contract of insurance;
- safeguarding and administering investments;
- sending dematerialised instructions;
- establishing collective investment schemes;
- establishing stakeholder pension schemes;
- providing basic advice on stakeholder products;
- advising on investments;
- advising on home finance activities;
- Lloyd's market activities;

- entering funeral plan contracts;
- entering into a home finance activity;
- administering a home finance activity;
- agreeing to do most of the above activities;

The "regulated activities" stated above must be carried on in respect to "specified investments" are defined in Part III of the RAO i.e.:

- deposits;
- electronic money;
- rights under a contract of insurance;
- shares;
- instruments creating or acknowledging indebtedness;
- sukuk (shariah compliant debt instruments);
- government and public securities;
- instruments giving entitlement to investments;
- certificates representing certain securities;
- units in a collective investment scheme;
- rights under a stakeholder pension scheme;
- rights under personal pension scheme;
- options;
- futures;
- contracts for differences;
- Lloyd's syndicate capacity and syndicate membership;
- rights under funeral plan contracts;
- rights under regulated mortgage contracts;
- rights under a home reversion plan;
- rights under a home purchase plan; and
- rights to or interests in anything that is a specified investment listed, excluding 'Rights under regulated mortgage contracts', 'Rights under regulated home reversion plans' and Rights under regulated home purchase plans.'

3. Carrying on Regulated Activities without a Licence

FSMA 2000, s 23(1) provides that a person who contravenes the general prohibition is guilty of an offence. Under FSMA 2000, s 26, the general consequences of such an 'authorisation offence' are that (subject to relief by the Court) an agreement made in contravention of the general prohibition is unenforceable against the other party (usually a consumer), who may also recover losses and monies paid under the agreement. However, FSMA 2000, s 26(4) provides that s 26 does not apply if the regulated activity in question is accepting deposits. Instead, there is separate and more limited provision as to the enforceability of agreements 'the making or performance of which constitutes, or is part of, [the regulated activity of] accepting deposits'. FSMA 2000, s 29 provides in part:

(i) If the depositor is not entitled under the agreement to recover without delay any money deposited by him, he may apply to the court for an order directing the deposit-taker to return the money to him.

(ii) The court need not make such an order if it is satisfied that it would not be just and equitable for the money deposited to be returned, having regard to the issue mentioned in subsection (iii).

(iii) The issue is whether the deposit-taker reasonably believed that he was not contravening the general prohibition by making the agreement.'

4. Supervisory Bodies - PRA & FCA

The PRA is responsible for the prudential regulation and supervision of banks, building societies, credit unions, insurers and major investment firms. In total the PRA regulates around 1,700 financial firms. The PRA's role is defined in terms of two statutory objectives to promote the safety and soundness of these firms and, specifically for insurers, to contribute to the securing of an appropriate degree of protection for policyholders.

In promoting safety and soundness, the PRA focuses primarily on the harm that firms can cause to the stability of the UK financial system. A stable financial system is one in which firms continue to provide critical financial services – a precondition for a healthy and successful economy.

The PRA makes forward-looking judgements on the risks posed by firms to its statutory objectives. Those institutions and issues which pose the greatest risk to the stability of the financial system is the focus of its work.

The PRA was created by the Financial Services Act (2012) and is a part of the Bank of England. It has close working relationships with other parts of the Bank, including the Financial Policy Committee and the Special Resolution Unit.

The PRA works alongside the FCA creating a "twin peaks" regulatory structure in the UK. The FCA's statutory objectives were established under FSMA as amended by the Financial Services Act 2012. The FCA's statutory objective is to ensure that the relevant markets function well. To support this, the FCA has three operational objectives:

- to secure an appropriate degree of protection for consumers;
- to protect and enhance the integrity of the UK financial system; and
- to promote effective competition in the interests of consumers.

5. Authorisation - FSMA

There are two principal ways of becoming an authorised person under FSMA. First, by exercising either rights under the EU Treaty or passporting rights under an EU Directive to carry on business in the UK on a services basis or an establishment basis (see comments below).

Second, by applying for and obtaining a FSMA Part 4A permission, which is the route to authorisation followed by domestic UK entities and entities incorporated outside of the EU. In the case of a domestic firm, therefore, authorisation under FSMA is obtained indirectly, by applying for permission to carry on specified regulated activities. The specific regulated activities for which each domestic or third country firm has permission, or which each incoming EEA firm is entitled to carry on in the UK, are published on the Financial Services Register, available online: http://www.fsa.gov.uk/register/home.do

Section 55(1) of FSMA provides that an application for authorisation for permission may be made to the appropriate regulator. Currently, the regulated activities of accepting deposits, effecting or carrying out contracts of insurance and the regulated activities specific to the operation of the insurance markets at Lloyd's of London have been designated as PRA regulated activities.

Authorisation by the PRA subjects a firm to regulation in the PRA in respect of matters relevant to the PRA's statutory objectives (see below), but does not relieve the firm of regulation by the FCA in respect of matters relevant to the FCA's separate statutory objectives (see below). Accordingly, FSMA uses the term PRA authorised person as short hand for a firm that is dual regulated by both the PRA and FCA.

Please see the following link which provides guidance on the application process of becoming licensed as a bank in the UK. It is published by the FCA: http://www.fca.org.uk/static/documents/banking-authorisation-process.pdf

6. Authorisation - Other licensable Activities

The carrying on of payment services (see below) and the issuing of electronic money is governed by secondary legislation which is distinct from FSMA.

(a) Payment Services Regulations

The Payment Services Regulations ("**PSR**") and parts of the FCA Handbook implement the Payment Services Directive in the UK. In general, these require payment service providers to be either authorised or registered by the FCA and to comply with certain rules about providing payment services, including specific requirements concerning payment transactions.

A credit institution will be subject to the conduct of business requirements in the PSRs to the extent that it provides payment services.

In the FCA's view, the authorisation process applying to UK and non-EEA credit institutions remains that imposed by Part 4A of FSMA (see above). Therefore, authorised credit institutions/banks will not though need to apply for a separate Part 4A permission, in order to provide payment services. In other words, if a UK credit institution/bank has a Part IV FSMA permission to carry on the regulated activity of accepting deposits, it will not need to be separately authorised to provide payment services in the UK. We are aware that the European Commission has indicated that branches of non-EEA credit institutions are unable to provide payment services in the EEA, in this legal form. In the FCA's view, however, the UK branch of a non-EEA credit institution with a Part 4A FSMA permission to accept deposits is also authorised to provide payment services in the UK

Authorised/registered payment service providers must comply with certain rules about providing payment services. The rules are set out in the PSRs. Additionally, such firms must comply with other areas of UK law, such as money laundering regulation and legislation.

In summary, the PSRs set out the following:

- An authorisation and prudential regime for payment service providers that are not banks, building societies or e-money issuers (and so already authorised or certificated by the FCA). Such businesses are known as authorised payment institutions ("**authorised PIs**"). Authorised PIs can passport their services to other EEA States – in other words, because of their UK authorisation, they have the right to establish or provide services across the EEA.

- Permit payment service providers operating beneath a certain average monthly turnover threshold to be registered instead of obtaining authorisation . Such small payment institutions are unable to passport.

- Exempt certain payment service providers (for example, banks, electronic money institutions) from authorisation/registration requirements (see comments above).

- Set out conduct of business requirements. In this context, this means requirements for information to be provided to payment service users, and specific rules on the respective rights and obligations of payment service users and providers. These requirements are applicable to all payment service providers with effect from 1 November 2009, whether they are payment institutions, banks, building societies, e-money issuers or any other category. In addition, banks and building societies need to comply with the Banking: Conduct of Business Sourcebook.

- Stipulate that rules governing access to payment systems should be non-discriminatory, subject to certain exemptions. This is aimed at supporting competition among payment service providers.

(b) E-Money Regulations

The Electronic Money Regulations 2011 ("**EMR**") implement the second Electronic Money Directive, which was adopted by the European Parliament and the Council of the European Union in September 2009.

While banks/credit institutions, credit unions and municipal banks require a Part 4A permission under FSMA of issuing electronic money (see above), where a firm is not a credit institution/bank but wants to issue electronic money, it must be licensed by the FCA. This licensing regime is not the same as the authorisation regime under FSMA. Rather, such a firm would need to obtain a licence from the FCA under the Electronic Money Regulations 2011.

As such, electronic money issuers are required to be either authorised or registered by the FCA (either as registered/authorised electronic money issuers or as FSMA firms with permission to issue electronic money).

Further, they must comply with certain rules about issuing e-money. The rules are set out in the EMRs, the PSRs and parts of the FCA Handbook as well as other areas of UK law such as money laundering regulation and legislation.

The EMRs set out:

- the definition of e-money and the persons that must be authorised or registered under the EMRs when they issue e-money;

- standards that must be met by EMIs for authorisation or registration to be granted;

- capital requirements and safeguarding requirements for EMIs;

- rules relating to issuing and redeeming e-money for all electronic money issuers; and

- the FCA's powers and functions in relation to supervision and enforcement in this area.

The PSRs contain conduct of business rules that are applicable to most electronic money issuers for the payment services part of their business.

The FCA Handbook sets out, among other relevant material:

- the requirements for certain electronic money issuers to submit returns;

- complaints handling procedures that electronic money issuers must have in place;
- the right of certain customers to complain to the Financial Ombudsman Service (the ombudsman service);
- the FCA's policy and procedures for taking decisions relating to enforcement action and when setting penalties;
- the FCA's ongoing fees; and
- levies for the ombudsman service and the Money Advice Service.

7. Controllers of a bank

Due to the influence that controllers have over firms, the PRA requires information in order to understand who owns or controls firms that its regulates. The PRA assess whether controllers, or potential controllers, of an authorised firm are suitable to act as a controller or will not prevent the PRA and the FCA from supervising the firm effectively.

A firm that is applying for permission to carryout one or more regulated activity, is required to complete and submit forms for its controllers and those which have "close links" to the applicant firm. A controller includes a person who holds 10% or more of the shares in an authorised firm or its parent undertaking and therefore may include certain shareholders of the applicant firm.

Approval must be obtained from the PRA before effecting a change in control. It is a criminal offence under section 191F of FSMA to acquire or increase control without notifying the PRA and receiving approval first. Inserting a holding company is considered a change in control event which the PRA must approve in advance, even though the ultimate controller is not changing.

A person is a controller if they hold:

- 10% or more of the shares in a UK-authorised person (A) or a parent undertaking (P) of A; or
- 10% or more of the voting power in A or P; or
- shares or voting power in A or P as a result of which they are able to exercise significant influence over the management of A.

A person must also seek approval from the PRA before it increases its control above the following thresholds:

- 10% or more but less than 20%;
- 20% or more but less than 30%;
- 30% or more but less than 50%;
- 50% or more; or
- Parent undertakings

The PRA also has the power to impose restrictions on a controller's shareholdings in an authorised firm or to apply to court for an order of a sale of shares, or the disposition of voting power.

Controllers must notify the PRA in writing of a reduction or cessation of control prior to effecting the change, although the PRA’s approval is not require

When assessing an application to become a controller, the PRA will consider the following:

- the reputation of the proposed controller;
- the reputation and experience of those who will direct the PRA authorised firm following the proposed acquisition or change of control.
- The financial soundness of the proposed controller, particularly in relation to the type of business that the PRA authorised firm pursues or intends to pursue.
- Whether the PRA authorised firm will be able to comply with applicable prudential requirements.
- If the PRA authorised firm will become part of a group following the acquisition, or increase of control, whether the group's structure enables the appropriate regulator to:

  a) exercise effective supervision;

  b) exchange information among regulators; and

  c) determine the allocation of responsibility among regulators.
- Whether there are reasonable grounds to suspect that any money-laundering or terrorist financing is being committed or attempted in connection with the proposed acquisition or increase in control, or whether the risk of such activity could increase

In addition to the above, the PRA (in consultation with the FCA) will consider the impact of a proposed change in control on the firm’s ability to comply and continue to comply with its prudential requirements, including the relevant threshold conditions. This may include, for example, the resilience of the target firm’s business model, capital and liquidity position, governance, risk management and controls, and the group structure.

We have focused on the notification requirements for a person obtaining or increasing its control over a firm that is authorised by the PRA, however, there are also ongoing requirements on the authorised firm in respect to their controllers, for example, they must monitor the identity of their controllers and make notifications to the PRA about their controllers in certain circumstances.

8. Permitted Activities and Restrictions

In general, banks are permitted to perform the services within the scope of their permissions granted by the PRA/FCA. This can extend beyond banking activities and can also includes non-regulated business. Banks are not required to apply for permission before carrying out non-regulated activities, however, as a part of their ongoing regulatory obligation they are required to notify the PRA of any significant change to their business.

Barclays Bank Plc has permissions to carry on the following regulated activities in the UK.

- accepting deposits;
- acting as trustee of an authorised unit trust;
- acting as trustee or depositary of an unauthorised alternative investment fund;
- administering a regulated mortgage contract;
- advising on investments;
- advising on pension transfers and pension opt outs;
- advising on regulated mortgage contracts;

- agreeing to carry on a regulated activity;
- arranging (bring about) deals in investments;
- arranging (bringing about) a home reversion plan;
- arranging (bring about) regulated mortgage contracts;
- arranging safeguarding and administration of assets;
- assisting in the administration and performance of a contract of insurance;
- causing dematerialised instructions to be sent;
- dealing in investments as agent;
- dealing in investments as principal;
- entering into a regulated mortgage contract as lender;
- establishing, operating or winding up a regulated collective investment scheme;
- establishing, operating or winding up a unregulated collective investment scheme;
- issuing electronic money;
- making arrangements with a view to a home reversion plan;
- making arrangements with a view to regulated mortgage contracts;
- making arrangements with a view to transactions in investments;
- managing investments;
- operating a multilateral trading facility;
- providing information in relation to a regulated benchmark;
- safeguarding and administration of assets (without arranging); and
- sending dematerialised instructions.

As you can see from the above, Barclays' permissions is the UK are broader than accepting deposits/banking business and include both insurance mediation, investment business and mortgage business. Please see below for a link to Barclays Bank Plc's 2013 Pillar 3 report.[7] This report contains information on how Barclays Bank Plc's meets its capital requirements and how consolidated reporting (see below) affects the Barclays Group: http://www.barclays.com/content/dam/barclayspublic/docs/InvestorRelations/AnnualReports/AR2013/barclays_pillar_3_report_2013.pdf

Please note that the UK regulators can impose limitations / restrictions on a firm which could affect how such regulated activities are performed.

---

7 Broadly, this is a requirement on banks which is aimed to complement the minimum capital requirements and supervisory review process by developing a set of disclosure requirements which will allow the market participants to gauge the capital adequacy of an institution. The aim of Pillar 3 is to allow market discipline to operate by requiring institutions to disclose details on the scope of application, capital, risk exposures, risk assessment processes, and the capital adequacy of the institution. It must be consistent with how the senior management, including the board, assess and manage the risks of the institution.

(a) Ring-Fencing

Please note that there are proposals which will restrict banking business in the UK. These are currently being consulted upon and relate to ring-fencing of certain activities (described below).

The UK Government has stated its intention for ring-fencing to take effect in the UK from 1 January 2019. The PRA intends to undertake further consultations during 2015 and to publish final rules and supervisory statements in 2016 to provide firms with sufficient time for implementation. We summarise these reforms below.

In response to the financial crisis, a number of domestic and international reforms to bank regulation have been introduced or are currently being implemented. Many of these reforms seek to improve the resilience and resolvability of banks, including through making changes to their structure.

In the United Kingdom, the Independent Commission on Banking ("**ICB**"), chaired by Sir John Vickers, made recommendations on how the UK banking system could be reformed to improve financial stability and increase competition. The ICB issued its final report in September 2011. It proposed, amongst other measures, the 'ring-fencing' of vital banking services from risks elsewhere in the financial system. This is intended to protect retail banking from risks unrelated to the provision of that service and ensure that banking groups which get into trouble can be resolved in an orderly manner, thereby avoiding taxpayer liability and ensuring the continuous provision of necessary retail banking services.

June 2012, the Government published a White Paper which set out proposals for the banking sector based on the ICB's recommendations, including those relating to ring-fencing and increasing banks' capacity to absorb losses. This formed the basis of draft legislation which was reviewed by the Parliamentary Commission on Banking Standard ("**PCBS**"). The Government's response to the PCBS, and its impact assessment, were published in February 2013.

The eventual legislation — the Financial Services (Banking Reform) Act 2013 — received Royal Assent in December 2013. The Act defines 'core activities' as the regulated activity of accepting deposits and requires that banking groups which undertake core activities place these activities into ring-fenced bodies ("**RFBs**"). To supplement the definition of core activities, the Act defines three 'core services'. These core services are:

- facilities for the accepting of deposits or other payments into an account which is provided in the course of carrying on the core activity of accepting deposits;
- facilities for withdrawing money or making payments from such an account; and
- overdraft facilities in connection with such an account. The PRA is required to discharge its general functions in a way that is consistent with its objectives relating to the provision of these core services.

The Act also prohibits RFBs from undertaking 'excluded' activities, and specifies that this includes dealing in investments as principal. More detail on the definition of core activities and RFBs, and the activities which RFBs can and cannot undertake, is set out in two pieces of secondary legislation made by HM Treasury in 2014.

- The Ring-fenced Bodies and Core Activities Order 2014 specifies that institutions which have more than £25 billion of core deposits from individuals and small businesses will be subject to ring-fencing requirements. It also provides for large organisations and high net worth individuals to place deposits outside RFBs if they so choose.
- The Excluded Activities and Prohibitions Order 2014 defines commodities trading as an excluded activity, and makes a number of activity prohibitions with which RFBs must

comply, such as incurring exposures to certain other financial institutions. A number of these exclusions and prohibitions are subject to exceptions.

In the European Union (EU), the European Commission has published a proposal for a regulation on structural measures improving the resilience of EU credit institutions in January 2014. The proposal included a ban on proprietary trading, and powers for supervisors to require the separation of other trading activities, including market-making, from deposit-taking within a banking group. This proposal has been submitted to the European Parliament and to the Council of the European Union. The outcome of this legislative process may affect elements of the PRA's implementation of ring-fencing.

(b) Indirect Restrictions

Banks/credit institutions are indirectly restricted from doing business through the following types of requirements:

- *Capital adequacy* - The purpose of setting aside capital is to enable a bank to absorb losses. The key elements of the capital adequacy framework for banks are:
  - first, a common definition of capital resources focussed on genuine loss absorbency in a going concern - Common Equity Tier 1;
  - second, a framework for capital which comprises minimum capital requirements and capital buffers, with the buffers varying in size depending on a bank's size and the nature of its activity and risk, and varying through the cycle;
  - third, using a combination of different approaches to assessing capital adequacy – risk-based approaches, stress tests, and a leverage ratio; and
  - fourth, within the risk-based approach, striking a balance which recognises the potential benefits of firms' internal models while guarding against their weaknesses and the incentive problems they create.

The amount of capital required depends on the kinds of assets the bank holds - generally, the riskier the asset, the more capital is required. If a bank does not comply with these requirements, it will face enforcement action and may need to cease business.

The capital requirements which UK banks must comply with stem from CRD IV, which is made up of the Capital Requirements Directive (2013/36/EU) ("**CRD**") which must be implemented through national law and the Capital Requirements Regulation (575/2013) ("**CRR**"), which is directly applicable to firms across the EU.

- *Liquidity* - Credit institutions/banks must invest their funds in a way as to ensure that adequate liquidity for payment purposes is guaranteed at all times. The liquidity risk is the danger that an institution cannot ensure its payment obligations. The CRR and PRA/FCA Rules contain detailed rules regarding liquidity.
- *Credit Risk* - The PRA Rules and the CRR contain detailed provisions regarding an institution's exposures.

(c) Specific scope of restricted business and restricted activities

There is no regulation that would restrict the businesses and activities of bank groups or financial holding groups. The main restrictions come from the prudential rules in the CRR. For further information see below 2.2 (e) of "Banking regulations and other - Germany".

9. Applicable Regulation

An authorised bank is required to comply with various UK rules and regulations including:

- FSMA;
- the PRA/FCA Rules - http://fshandbook.info/FS/ ;
- Money laundering and terrorist financing laws and regulations;
- to the extent relevant, the Payment Services Regulations 2009, the Electronic Money Regulations 2011, Consumer Credit Act 1974;
- EU regulations which have direct effect in the UK; and
- non-financial services legislation and regulation including, amongst other things, consumer protection and data protection laws and regulations (which are mentioned in further detail below).

Additionally, the FCA has statutory powers to give guidance consisting of such information and advice as the FCA considers appropriate in respect to any matters including parts of FSMA and any rules made by the FCA. Authorised banks should also consider and comply with such requirements.

10. Financial Promotion / Marketing Rules

A substantial part of the FCA's conduct of business regulation under FSMA is directed at ensuring that the information provided by authorised firms to customers about financial products and services is fair, clear and not misleading. The aim is to ensure that customer choice as to whether or not to enter into a new relationship with a financial services providers (such as a bank).

The "financial promotion" regime in section 21 of FSMA provides that a person must not, in the course of business, communicate an invitation or inducement to engage in investment activity. To engage in investment activity means to enter or offer to enter into an agreement the making or performance of which by either party constitutes a controlled activity or to exercise any rights conferred by a controlled investment to acquire, dispose of, underwrite or convert a controlled investment. The range of controlled activities and controlled investments is specified in subordinate legislation under FSMA, in particular the Financial Services and Markets Act 2000 (Financial Promotion) Order 2005 ("**FPO**").

Article 4 of the FPO provides that controlled activities are those which fall within the FPO, Schedule 1, paragraphs 1 to 11; and that controlled investments are those investments that fall within any of FPO, Schedule 1 paragraphs 12 to 27. Article 2 of the FPO states that a deposit means a sum of money which is a deposit for the purposes of Article 5 of the RAO. FPO Schedule 1 then defines deposit as a controlled investment and FPO Schedule 1, paragraph 1 provides that accepting deposits is a controlled activity if:

(i) money received by way of deposit is lent to others; and

(ii) any other activity of the person accepting a deposit is financed wholly, or to a material extent, out of the capital of or interest on money received by way of deposit.

and the person accepting the deposit holds himself out as accepting deposits on a day-to-day basis.

Therefore, in respect to banking business, the scope of the FPO is congruent to the scope of deposit taking in the RAO.

In summary, therefore, to promote a deposit taking business in the UK (including by making or causing to be made from outside the UK, a communication capable of having effect in the UK) is in principle within the scope of the financial promotion restriction. Such a promotion is an offence unless there is an available exclusion from the scope of the restriction. In addition an unlawful promotion renders any resulting agreement with (or exercise of rights by) a consumer unenforceable against the consumer and confers on the consumer a right to recover money or property transferred and to claim damages, unless the Court is satisfied that it is just and equitable to enforce the agreement.

The most obvious available exclusion from the financial promotion restriction appears in FSMA, section 21(2), which provides that the restriction does not apply if either the promotion is made by an authorised person (i.e., a person with authorisation and permission under FSMA) or the content of the promotion is approved for the purposes of FSMA section 21 by an authorised person. In addition, pursuant to section 21 of FSMA, the FPO provides a range of detailed exclusions from the scope of the financial promotion restriction, the availability of which will depend on the facts of the particular case.

11. EU Passporting Regime

A UK-authorised firm may be eligible to carry out its permitted activities in another EEA Member State if it fulfils the requirements under the scope of the relevant single market directive. This is also the case if an EEA authorised firm wishes to carry on activities in the UK. This eligibility is referred to as an ‘EEA right’ and exercising this right is known as ‘passporting’.

An eligible firm may choose to either:

(i) establish a presence in another EEA Member State, (the ‘host’ state), known as an ‘establishment’ passport, or

(ii) carry out its permitted activities cross-border, without establishing a presence in the host Member State, referred to as a ‘services’ passport

A UK-authorised firm that is dual-regulated (by both the FCA and PRA) and wishes to exercise its passporting rights must notify the PRA of its intention to do so. A solo-regulated firm must notify the FCA. The notification must provide the information set out in the applicable single market directive and include whether the intention is to set up an establishment or provide services into the host state.

The activities that are "passportable" are set out in the relevant EU directives. The relevant EU directives are as follows:

- Insurance Mediation Directive (IMD);
- Markets in Financial Instruments Directive (MiFID);
- Undertakings for Collective Investment in Transferable Securities Directive (UCITS);
- Payment Services Directive (PSD);
- Second Electronic Money Directive (2EMD);
- Alternative Investment Fund Managers Directive (AIFMD);
- Capital Requirements Directive (CRD IV);
- Third Non-Life Insurance Directive;
- Consolidated Life Assurance Directive, and
- Reinsurance Directive.

Activities that are not covered by the directives are not passportable. A firm wishing to carry on such activities would need to contact the relevant competent authority of the host state to seek direct authorisation for these activities. For example, please note that currently there is no specific passporting regime for consumer credit activities. This means that a bank can passport the activity of consumer lending under the Capital Requirements Directive but a non-bank lender cannot provide consumer lending services in other EEA States without obtaining a separate licence in the relevant Member State.

Any subsequent changes to the original notification details, such as change of address, management or organisational structure, must be notified to the FCA or PRA before the change is implemented (unless there are circumstances beyond the firm's control), in accordance with the Treasury Passport Regulations.

An authorised UK firm that holds the relevant permissions has a right to carry on business in another EEA state, providing the requirements of the single market directive under which the activities will be carried out are met. Please note that authorised branches of third country firms are not eligible to passport their services.

There are 29 (not including the UK) EEA States with passporting rights: Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden. Please note, however that although the whole of Cyprus became part of the EU in May 2004, EU legislation only applies to the Republic of Cyprus (the Southern part of the island) and so passporting rights only exist to this extent.

Please note that the single market directives do not apply in the Channel Islands or the Isle of Mann, even though they are Crown dependencies. This means that firms based in these territories are treated in the same way as firms based in a non-EEA State and do not have passporting rights under the FSMA single market directives. Similarly, UK firms do not have passporting rights in relation to the Channel Islands and the Isle of Man. As such, UK firms will have to apply direct to the relevant financial regulators in each territory for permission to conduct business there. The FSA has no formal involvement in this process (although we would expect firms to keep supervisors here informed of their activities). Gibraltar enjoys a separate status to the Channel Islands and Isle of Man and the single market directives apply to it in full. However, passporting rights apply only between EEA States and so passporting rights between Gibraltar and the UK do not apply. Instead the UK and Gibraltar have agreed special arrangements under the Gibraltar Order.

Switzerland is not an EEA State and so there are no passporting rights under the single market directives. That said, EEA general insurers do have the right to set up an establishment in Switzerland (and vice versa) under the provisions of special bilateral treaties between the European Union and Switzerland. However, it is important to note that this is not a passport right – a Swiss general insurer will still need to obtain Part IV permission to set up an establishment in the UK (although paragraphs 3 to 5 of Schedule 6 of the FSMA (the threshold conditions relating to close links, adequate resources and suitability) would not apply in relation to such an establishment, and it would not need an additional permission for insurance mediation).

Generally speaking and in terms of supervision, where a firm passports its activities using a services passport, it will be subject to the supervision of its home state regulator. However, where a firm passports using an establishment passport, it will be subject to home state regulator rules in areas such as conduct of business and liquidity.

12. Supervision of overseas firms operating in the United Kingdom - PRA

The PRA's supervision of overseas firms operating in the United Kingdom reflects an assessment of the potential impact of the UK entity on UK financial stability, including via risks from overseas, its legal status (branch or subsidiary), the nature of the home country regulatory regime (where the firm originates from a non-EEA country) and whether or not the firm is a G-SIFI.

- *For subsidiaries of overseas firms authorised by the PRA* - The PRA has full powers and responsibilities and so its approach is to treat such firms equivalently to UK-owned firms (applying its full prudential requirements, including for example stress testing for the most significant firms). Consistent with its objective the PRA assesses, and limits as necessary, the (potentially complex) inter-linkages with the rest of the group.

- *For UK bank branches of EEA firms* - The PRA's powers and responsibilities are limited under European law. In order to assure itself that risks to the UK financial system from such branches are adequately managed, the PRA focuses on resolution planning (along with the SRU) and on ensuring that it has access to relevant information on the safety and soundness of the parent firm via collaboration with home regulators. In particular the PRA engages in supervisory and resolution colleges, including Crisis Management Groups ("**CMGs**") where applicable. The PRA takes a close interest in liquidity, focusing, in collaboration with the home regulator, on the position of the whole firm of which the branch is a part. The PRA expects UK branches of EEA firms to appoint a senior individual with authority to act as a primary contact with the PRA in relation to the branch's affairs. This individual should also act as a channel for communication with the parent. Where the PRA is not satisfied regarding the safety and soundness of the branch and the parent firm, it works with the home authority and promotes public understanding of the limits of its powers, and uses whatever tools it can to reduce the impact of these limitations. In emergency situations, consistent with European law, the PRA will take any precautionary measures necessary to protect the interests of depositors, and will inform the home authority of such measures at the earliest opportunity. In some cases, the PRA may judge that an EEA firm applying to passport into the United Kingdom poses risks to its objective, but does meet the requirements set out by the relevant EU Directives, and thus as a legal matter has a right to conduct business in the United Kingdom. In such cases, the PRA will carefully consider the tools available to it as a host regulator, acting in co-operation with the home regulator, to mitigate the resulting risks.

- *For UK branches of non-EEA firms authorised by the PRA* - The PRA's authorisation applies to the whole firm. At the point at which a non-EEA branch seeks initial authorisation in the United Kingdom, the PRA will, as a first step, form a judgement on the adequacy of the home regulator, including its ability and willingness to share confidential information. Where it considers the home supervisor not to have a regime broadly equivalent to that of the United Kingdom, the PRA will refuse authorisation of the branch. It may instead decide to authorise a stand-alone subsidiary, in which case it may limit the inter-linkages with the rest of the group or ring-fence the subsidiary (for example if it considers the home supervisor not to deliver effective consolidated supervision). In assessing a non-EEA firm against the Threshold Conditions (i.e., the conditions a firm must fulfil in order to become authorised and on an on-going basis), the PRA may also have regard to the opinion of an overseas regulator in a country in which the firm carries on regulated activities. In considering how much weight to attach to such opinions, the PRA must have regard to the nature and scope of the supervision exercised by the overseas regulator. For existing UK branches of non-EEA firms where the home regime is not considered to be equivalent, the PRA's supervisory work is aimed at mitigating the risks of non-equivalence in the relevant areas. Its supervision focuses on issues such as the financial strength of the whole firm, including the adequacy of its liquidity and the resolution plan for the firm (collaborating with the SRU and home authorities to develop such plans in colleges or CMGs as applicable), taking into account the importance of the firm to the PRA's objective. For UK branches of non-EEA firms where the PRA is satisfied that the home regulatory regime is equivalent, and where the PRA has assured itself over resolution plans and the home regulator's supervisory approach, the PRA relies where possible on the home regulator's prudential supervision. In these cases, the PRA focuses on collaboration with home regulators (including via supervisory colleges) and on resolution plans. In addition, the PRA takes a close interest in liquidity and ensures that there are senior individuals in the United Kingdom that are clearly responsible for management of both the UK operations and business booked in the United Kingdom. The PRA discusses and agrees with the home regulator the areas in which it will seek to rely on the home regulator's supervision.

We understand that under Japan's Banking Act, Japanese banks are able to act as an agent for the provision of banking services by foreign banks to Japanese customers. Accordingly, when providing services through Japanese banks, foreign banks are exempt from the normal licensing requirements. There is no equivalent exemption in the Untied Kingdom. However, as discussed above, there is an exemption from the financial promotion restriction if either the promotion is made by an authorised person or the content of the promotion is approved for the purposes of FSMA section 21 by an authorised person. Accordingly, a foreign bank can make a financial promotion to a UK resident if the financial promotion is approved by a UK authorised person.

13. Restrictions on Bank Groups, Bank Holding Company Groups and Financial Holding Company Groups

(a) Consolidated Supervision

Broadly, an PRA/FCA authorised firm is subject to consolidated supervision if it is in a group that contains more than one regulated financial firm and/or a holding company.

Being inside a consolidated group has an impact on a firm's capital and capital requirement calculations as well as their reporting requirements. Additional, being inside a consolidation group can extend the application of regulatory rules regarding remuneration (which apply to certain types of authorised firms, including banks) to the rest of the consolidation group.

The definition of what constitutes a "UK consolidation group" is complex. The rules are contained in the PRA/FCA Rules at BIPRU 8: http://fshandbook.info/FS/html/handbook/BIPRU/8 . In order to consider whether or not a UK authorised firm is part of a UK consolidation group, you need to assess whether the firm and its parent or subsidiary undertakings fall within specific definitions. These definitions stem from EU legislation.

(b) Financial Conglomerates

Financial conglomerates are large financial groups, or sub-groups, that operate in the insurance sector and in the banking and/or investment services sector. Because of their size and complexity, financial conglomerates are often of systemic importance to individual EU member states or the EU as a whole.

The Financial Conglomerates Directive ("**FICOD**") introduced a prudential regime for financial conglomerates in order to combat problems arising from the risks associated with large cross-sector businesses. FICOD provides for a supplementary supervisory framework for financial conglomerates to be applied in addition to requirements set out in sectoral directives, specifically:

- CRD IV; and
- the Insurance Groups Directive.

FICOD provides for:

- Enhanced co-operation processes (including information sharing) between cross-sector and cross-border supervisors of financial conglomerates, including the appointment of a single lead regulator to act as a co-ordinator for, and to exercise supplementary supervision over, each financial conglomerate.

- Supplementary capital adequacy requirements for certain entities within a financial conglomerate.

- Supplementary supervision of risk concentrations and intra-group transactions.

- Requirements for the vetting of persons having effective control over the business of a financial conglomerate.

Very broadly, a financial conglomerate is a group of entities whose primary business is financial and whose regulated entities engage to a significant extent in at least two of the activities of banking, insurance and securities. The definition of financial conglomerate for the purposes of the FICOD and UK law is extremely complex and is set out in Articles 2 and 3 of the FICOD. These have been implemented in the UK in General Prudential Sourcebook ("**GENPRU**" - http://fshandbook.info/FS/html/handbook/GENPRU) of the PRA/FCA Handbook and the decision tree set out in GENPRU 3 Annex 4R.

Competent authorities that have authorised regulated entities are responsible for identifying whether a group, or sub-group, is a financial conglomerate. When a financial conglomerate is identified, the authority appointed as the co-ordinator supervisor (or lead regulator) for the financial conglomerate must inform the parent undertaking that heads the group (or, if there is no parent undertaking, the regulated entity with the largest balance sheet total in the most important financial sector of the group) that the group has been identified as a financial conglomerate. It must also notify the Joint Committee of the European Supervisory Authorities ("**ESAs**"). See below for a link to a list of financial conglomerates as of 31 July 2013: http://www.esma.europa.eu/system/files/jc_2013_055_identification_of_financial_conglomerates_v2.pdf

Generally speaking, financial conglomerates are subject to additional supervisory requirements, referred to in the FICOD as "supplementary supervision", relating to:

- Capital adequacy;

- Intra-group transactions and risk concentrations;

- Organisational requirements;

Additionally, supplementary supervision applies to every regulated entity which is:

- At the head of a financial conglomerate.

- Part of a financial conglomerate, the parent undertaking of which is a "mixed financial holding company"[8] that has its head office in the EU.

- Linked with another financial sector entity through a consolidation relationship.

If a group has its head office outside the EU, the FICOD requires the supervisor who would be the group's co-ordinator (if it were based in the EU) to verify whether the group is subject to supervision equivalent to that provided by the FICOD. If there is no equivalent supervision, member states must apply (by analogy) FICOD's provisions concerning supplementary supervision of regulated entities. Alternatively FICOD allows supervisors to apply other specified methods to ensure appropriate supplementary supervision. These include establishing a mixed financial holding company with its head office in the EU and then applying supplementary supervision to the new sub-group.

(c) Power to Direct "Qualifying Parent Undertakings"

[8] In summary, this is defined as an undertaking which is not a regulated entity but which heads a financial conglomerate.

Statutory provisions relating to the power of direction are set out in sections 192A to 192I FSMA. Broadly, these provisions permit the PRA and FCA to impose directions on "qualifying parent undertakings" of certain FSMA authorised firms to take specific actions (e.g., to inject capital).

Failure to comply with a direction can result in enforcement action being taken directly against the "qualifying parent undertaking".

In order for the PRA to be able to exercise the power of direction:

(i) the parent undertaking must be a 'qualifying parent undertaking' of a 'qualifying authorised person'; and

(ii) either the 'general condition' or the 'consolidated supervision condition' must be satisfied.

A parent undertaking is a 'qualifying parent undertaking' of a 'qualifying authorised person' under section 192B FSMA, if:

(i) it is the parent undertaking of a 'qualifying authorised person' (a 'qualifying authorised person' being a UK-incorporated body corporate that is an authorised person, and is either a PRA-authorised firm or an investment firm);

(ii) it is incorporated in the United Kingdom or has a place of business in the United Kingdom;

(iii) it is not itself an authorised person, recognised investment exchange or recognised clearing house; and

(iv) it is a financial institution of a kind prescribed by the Treasury by Order.

In relation to (iv) above, the Treasury has made an Order prescribing what is a 'qualifying parent undertaking'. The Order provides that the following are prescribed as 'qualifying parent undertakings':

(i) *insurance holding companies* — broadly, companies whose main business is to acquire and hold subsidiary companies which are exclusively or mainly insurance or reinsurance companies;

(ii) *financial holding companies* — broadly, companies whose principal activities are to acquire subsidiary companies which are either exclusively or mainly credit institutions, investment firms or financial institutions; and

(iii) *mixed financial holding companies* — companies which have at least one subsidiary which is a credit institution, an insurance undertaking or an investment firm and which, together with their subsidiaries, constitute a financial conglomerate for the purposes of the Financial Conglomerates Directive (see above).

In prescribing these categories of firms as 'qualifying parent undertakings', the Treasury has sought to bring within the scope of the power of direction those entities which are within the scope of consolidated (or supplementary) supervision under EU law (under CRD IV and the Financial Conglomerates Directive).

The definition of 'qualifying parent undertaking' includes any UK-incorporated parent undertaking (or parent undertaking with a place of business in the United Kingdom) in an ownership chain which meets the definitions contained in the Order, even if the undertaking is not itself the ultimate parent undertaking. In general, the PRA would consider action to be most effective when taken in relation to the ultimate parent undertaking at the head of the ownership chain, as that is usually where most of the power to direct and control the group resides.

However, where the ultimate parent undertaking is not a ‘qualifying parent undertaking’ (for example if the group is headed by a non-UK entity or a non-financial entity) then the PRA will not have the power to direct that ultimate parent undertaking. In such circumstances, the PRA may consider that use of the power of direction over another qualifying parent undertaking in the ownership chain is appropriate.

The PRA can only use the power of direction if either the general condition or the consolidated supervision condition is satisfied:

- **General condition** — the general condition is that the PRA considers that it is desirable to give the direction in order to advance, in the case of the PRA, any of its objectives. The PRA’s general objective is to promote the safety and soundness of PRA authorised firms. FSMA requires the PRA to advance this objective primarily by seeking to (a) ensure that the business of PRA-authorised firms is carried on in a way which avoids any adverse effect on the stability of the UK financial system; and (b) minimise the adverse effect that the failure of a PRA-authorised firm could be expected to have on the stability of the UK financial system. The PRA considers that these objectives will be advanced by having suitable requirements (for example, prudential standards or systems of governance and controls) enforced directly at group level. Where action to advance PRA objectives taken at the authorised firm level is considered to be, or likely to be, less effective than action taken at the qualifying parent undertaking level then the PRA will consider using its power of direction over the qualifying parent undertaking.

- **Consolidated supervision condition** — The consolidated supervision condition is that: (i) the PRA is the competent authority for the purpose of consolidated supervision that is required, in relation to some or all of the members of the group of a qualifying authorised person, in pursuance of any of the relevant EU directives; and (ii) the PRA considers that the giving of the direction is desirable for the purpose of the effective consolidated supervision of the group.

The PRA’s obligation to conduct consolidated supervision arises from the relevant EU Directives (e.g., the Banking Consolidation Directive and the Financial Conglomerates Directive) which in turn implement the relevant international standards on consolidated supervision (in particular the standards on consolidated supervision set by the Basel Committee on Banking Supervision in its Core Principles for Effective Banking Supervision, the International Association of Insurance Supervisors’ Insurance Core Principles and the Joint Forum Principles for the Supervision of Financial Conglomerates.

The PRA considers that the purpose of consolidated supervision is to enable supervisors to take necessary action to protect authorised firms from the adverse effects of being part of a group. These adverse effects may include: financial contagion (losses in a group entity impacting on a firm through financial linkages); reputational contagion (an event in one entity impacting adversely on another entity in the group through reputation damage); multiple gearing (i.e. use of the same capital resources more than once in the same group); upgrading the quality of capital within a group (i.e. by using funds borrowed by the parent undertaking to create core equity Tier 1 capital within the authorised firm, giving a false appearance of the quality of capital within a firm); barriers to effective resolution (e.g. complex group structures or intra-group arrangements); and the impact of intra-group relationships on authorised firms (exposures, contingent liabilities etc.)

The application of rules on prudential standards and systems of governance and control on a consolidated basis aims to address many of the risks above. Therefore, where the effectiveness of consolidated supervision would be greater if action was taken by the qualifying parent undertaking then the PRA will consider using its power of direction. For example, a particularly strong case for using the power of direction would be made where any act or omission of a qualifying parent undertaking leads, or could lead, directly or indirectly, to an authorised firm being unable to ensure compliance with rules applied at the consolidated level required by the relevant European legislation.

In determining whether there is compliance, the PRA will also take into account the purpose of the rule and its intended effect.

A direction placed on a qualifying parent undertaking regarding consolidated supervision will generally support the authorised firms in complying with their obligation to ensure that their consolidation group complies with consolidated requirements, but it will not absolve them of this obligation. In such circumstances action can be taken at both the qualifying parent undertaking and authorised firm level if necessary.

Please be aware that the FCA has the same powers and is permitted to use such powers with the proviso that it can only use the power of direction if either the general condition (i.e., that it is desirable to give the direction in order to advance one or more of its operational objectives) or the consolidated supervision condition is satisfied.

For the FCA, the consolidated supervision condition is that:

(i) the FCA is the competent authority for the purpose of consolidated supervision that is required, in relation to some or all of the members of the group of a qualifying authorised person, in pursuance of any of the relevant EU directives; and

(ii) the FCA considers that the giving of the direction is desirable for the purposes of the effective consolidated supervision of the group.

14. Customer Protection measures (only in respect to non-financial businesses regulations)

Outside of the banking and payment services sector, general consumer protection rules apply. Consumer protection law is currently undergoing a radical change in the UK to consolidate all of the sources of UK consumer law into one single act, currently known as the "Consumer Rights Bill". This Bill is expected to be passed into law by October 2015. Under the current law, there is no single definition of the term 'consumer'.

Below we outline the main consumer protection law sources with a brief overview of each one.

(a) Sale of Goods Act 1979

The Sale of Goods Act 1979 ("**SGA**") governs contracts for the sale of goods. It implies certain terms as to nature of the goods sold and as to performance of the contract. Many of the consumer-specific terms of the SGA will be replaced by the Consumer Rights Bill, when enacted. The SGA implies terms into contracts relating to the goods under the contract and to the performance of the contract.

Conditions implied relating to goods include:

- the seller has the right to sell the goods;
- the goods correspond with the description; and
- that the goods are of satisfactory quality.

Conditions implied relating to performance relate to where the relevant matters of performance are not expressly dealt with in the contract and there is no evidence of the parties' intentions. The intentions of the parties under the SGA is determined using a set of statutory rules.

These implied terms include:

- where no price for the goods is agreed, the price must be a reasonable one; and

- if no mention is made of when title in goods passes to the consumer, it is deemed to pass when the goods become ascertained and the parties intend it to pass.

(b) Supply of Goods and Services Act 1982

The Supply of Goods and Services Act 1982 ("**SGSA**") governs contracts for services, including goods transferred under a contract for services. The SGSA implies three terms into contracts for services, whether or not goods are transferred as part of the contract. Many of the consumer-specific terms of the SGSA will be replaced by the Consumer Rights Bill, when enacted.

(c) The Unfair Contract Terms Act 1977 (UCTA)

The Unfair Contract Terms Act 1977 ("**UCTA**") applies to contract terms or notices that seek to limit or exclude liability. It applies to contractual liability (contract terms) and tortious liability (notices). Under UCTA, different controls apply according to the nature of the liability that a supplier wishes to exclude or restrict. Very broadly, certain types of liability can never be excluded or limited in a consumer contract. However, other types of liability may be excluded or limited in a consumer contract, but only in so far as this satisfies the reasonableness test .When the Consumer Rights Bill is enacted, UCTA will be partially amended so that the rules relating to consumer contracts will move into the Bill and be merged with those in the UTCCRs .

(d) Cancellation of Contracts made in a Consumer's Home or Place of Work etc. Regulations 2008 - for contracts made on or before 12 June 2014

The Cancellation of Contracts made in a Consumer's Home or Place of Work etc. Regulations 2008 ("**Doorstep Regulations**") implement the Doorstep Selling Directive, a minimum harmonisation directive.

The Doorstep Regulations give consumers a right to cancel a contract that they enter into away from a seller's place of business (for example, during a trader's visit to the consumer's home, workplace or outside a local shopping centre) (doorstep selling). They do not require the consumer to give a reason for the cancellation. The cancellation period is seven calendar days from the receipt of the notice of the right to cancel.

(e) Consumer Protection from Unfair Trading Regulations 2008

The Consumer Protection from Unfair Trading Regulations 2008 make a seller criminally liable for misleading or aggressive sales practices. They also implement the Unfair Commercial Practices Directive ("**UCPD**"). The UCPD is a maximum harmonisation Directive (although it does permit more restrictive rules for financial services and immovable property).

(f) Provision of Services Regulations 2009

Business providing services in the UK must comply with the Provision of Services Regulations 2009 ("**POS Regulations**"). The POS Regulations will apply to the majority of private sector businesses in the UK providing services to consumers.

Under the POS Regulations, a seller must:

- provide consumers with certain information about itself;
- deal with customer complaints promptly;
- not discriminate against consumers in the provision of services on the basis of place of residence (unless such different treatment can be objectively justified).

(g) The Consumer Rights (Payment Surcharges) Regulations 2012

The Consumer Rights (Payment Surcharges) Regulations 2012 place a ban on charging consumers excessive fees for the use of payment methods. The Payment Surcharges Regulations implement Article 19 of the Consumer Rights Directive into UK law.

The ban on excessive payment surcharges applies if:

- a consumer is making use of a payment method for the purposes of a contract with a trader;
- the contract is for goods, services or digital content;
- the contract in respect of which payment is being made is not an excluded contract;
- the temporary exemption for micro-businesses does not apply.

(h) Unfair Terms in Consumer Contracts Regulations 1999

The Unfair Terms in Consumer Contracts Regulations ("**UTCCRs**") implement the Directive on Unfair Terms in Consumer Contracts ("**Unfair Terms Directive**"). When interpreting the UTCCRs, the courts will have regard to the Unfair Terms Directive, and interpret the UTCCRs in the light of this.

The Unfair Terms Directive is a minimum harmonisation directive therefore the UK was free to implement stricter consumer protection rules than those set out in the Unfair Terms Directive.

The UTCCRs:

- apply to unfair terms in contracts between a consumer and a seller of goods or services. A seller can include a public authority;
- apply to terms that are "not individually negotiated";
- require the seller to ensure that any written term is expressed in plain and intelligible language;
- impose a test of fairness. However, the fairness test does not apply to certain terms;
- include an indicative and non-exhaustive list of potentially unfair terms Provide that if a term is unfair, then it is not binding on a consumer, although the remainder of the contract shall continue in force if it is capable of doing so. The offending unfair term cannot be rewritten by the court, for example an unfair penalty term cannot be reduced by the court to make it fair.

Broadly speaking, a seller has to comply with the requirements of the UTCCRs as to form or style of drafting and also as to the substance of a term.

(i) Equality Act 2010

Sellers of goods and services (including facilities) to consumers must comply with the rules against discrimination, harassment and victimisation set out in the Equality Act. This act consolidates and expands on previous anti-discrimination legislation before that date.

15. Others

Using intermediaries in the UK, such as introducing brokers, investment advisers and asset managers will bring considerations of UK agency law. The appointment of third parties may also trigger outsourcing requirements.

(a) Cash Pooling

A clear distinction must be drawn between the services provided by the bank in the context of a cash management system and the services provided by the cash pool leader and by the participating members of the cash pool.

By providing the necessary accounts and by providing an over draft credit facility or operating credit line, the bank will be engaged in deposit business and lending business. Both activities require a banking license. No separate license for "cash management" services exists. Also, the bank is likely to provide payment services in connection with its cash management services.

As regards the cash pool leader and the cash pool members, the situation is similar, because when the cash pool leader makes a loan to the cash pool member it will be engaged in lending business. At the same time the cash pool member will be operating a deposit business. The same is true vice versa when the cash pool member deposits excess cash with the cash pool leader. In this case the cash pool leader will be operating a deposit business while the cash pool member may be engaged in lending business. However, all members of the cash pool including the cash pool leader will normally be exempt from the requirement of a banking license due to the fact that the FSMA contains a intragroup exemption. In summary, there is an exemption under UK law for various intra-group treasury services.

(b) Banking Front Services

We understand that this means that the provider has no regulatory licence but partners with a licensed/authorised bank to provide services to customers such as debit cards and ATMs.

In the UK, there are co-branded debit and credit cards in the market. These are issued by authorised banks, electronic money institutions or payment institutions (e.g., American Express). In such cases, it is the authorised firm which will issue the card and be subject to the applicable regulations (e.g., the FCA Rules, PSRs, Consumer Credit Act 1974 and other consumer legislation). The co-brand partner may offer a loyalty programme alongside the card (e.g., British Airways). In such cases, the co-brand partner may need to be authorised for intermediary activities such as credit brokerage (where the card is a credit card). Also, if the co-brand partner advertises and markets the card, it may need to comply with specific marketing rules (e.g., specific marketing rules exist under the consumer credit regime in the UK).

In all cases, the role of the non-licensed provider/entity will need to be carefully considered as its activities may:

(i) trigger a licensing requirement in the UK; and

(ii) trigger UK marketing / financial promotion laws.

Whether this will be the case will need to be considered on a case-by-case basis as it will depend on the specific activities of the provider and the relevant financial services/products being offered.

PAYMENT SERVICES - GERMANY

1. Glossary

German term	explanation	abbreviation
	Point of Sale	POS
	Directive 2007/64/EC on payment services in the internal market	PSD
Zentraler Kreditausschuss	German Central Credit Committee	ZKA
Deutsche Kreditwirtschaft	German Credit Industry	DK
Deutsche Bundesbank	German Central Bank	Bundesbank
	Real-time gross settlement system of Bundesbank	RTGSplus
	automated teller machine	ATM
Bürgerliches Gesetzbuch	German Civil Code	BGB
Zahlungsdiensteaufsichtsgesetz	German Payment Services Supervision Act	ZAG
	Single Euro Payments Area	SEPA
	all national central banks and the European Central Bank	Eurosystem
	European Union	EU
	European Central Bank	ECB
	Business Identifier Code	BIC
	International Bank Account Number	IBAN
Geldkarte	money card	
Landesbank	regional bank	
Hausbankverfahren	house bank procedure	HBV
	Second generation Trans-European Automated Real-time Gross Settlement Express Transfer System	TARGET2
Elektronischer Massenzahlungsverkehr	mass payment clearing system of Bundesbank	EMZ
TARGET2-Bundesbank	national TARGET system of Bundesbank	TARGET2-BBk
	Real Time Gross Settlement System	RTGS
	Information and Control Module	ICM
	European Economic Area	EEA
	Personal Identification Number	PIN
Geldautomaten-System	ATM system	
Sofortüberweisung	immediate credit transfer	
	European Payments Council	EPC
	Directive 2009/110/EC on the taking up, pursuit and prudential supervision oft he business of electronic money institutions	Second E-Money Directive
Einführungsgesetz zum Bürgerlichen Gesetzbuche	Introductory Law to the German Civil Code	EGBGB
Kreditwesengesetz	German Banking Act	KWG
Bundesanstalt für Finanzdienstleistungsaufsicht	German Federal Financial Supervisory Authority	BaFin
	payment services providers and e-money issuers together	institutions
Allgemeine Geschäftsbedingungen	General Terms and Conditions	AGB
ZAG-Anzeigenverordnung	ZAG Notification Regulation	
	Anti Money Laundering	AML
	Money Laundering	ML

	Counter Terrorist Financing	CTF
	Terrorist Financing	TF
	undertaking for collective investment in transferable securities, mutual funds complying with EU harmonized rules	UCITS
Unterlassungsklagegesetz	Cease and Desist Action Act	
	Short Message Service	SMS
Bundesdatenschutzgesetz	Federal Data Protection Act	BDSG
Geldwäschegesetz	Money Laundering Act	GWG
	Date Protection Authorities	DPA
Abgabenordnung	German Tax Code	
Strafprozessordnung	German Code of Criminal Procedure	
Telemediengesetz	Information Society Services Act	TMG
ZAG-Instituts-Eigenkapitalverordnung	Capital Adequacy Regulation for Payment Services and E-money Institutions	ZIEV
Geschäftsbesorgungsvertrag		
	Transaction Authentication Number	TAN
Mindestanforderungen an das Risikomanagement	The Minimum Requirements for Risk Management	MaRisk
Bundesamt für Sicherheit in der Informationstechnologie	German Federal Office for Information Security	BSI
IT-Grundschutz-Kataloge	catalogues on basic protection of IT systems	
Bundesdatenschutzgesetz	Federal Data Protection Act	BDSG
	virtual private network - connection	VPN-connection
	politically exposed person	PEP
	Electronic Banking Internet Communication Standard	EBICS
	Home Banking Computer Interface	HBCI
	Financial Transaction Services	FinTS

2. Overview over monetary flow

2.1 Brief historical development of pre-SEPA payment systems in Germany

Historically, money payments in Germany were mostly account-based payment flows that companies and individuals have used to pay their bills. The larger part of such credit transfers have historically always been "push" payments, but also to a significant extent "pull" payments (direct debits) initiated by the payee.

Payments by cheque have never played a particularly large role (compared to, for example, France). Payments in stores used to be mainly cash-based. In the 1970s and 1980s, when an increasing number of payments in stores were made on a non-cash basis, the Euro cheque system enjoyed a brief period of success. If the issuer of the cheque presented a matching Euro cheque card and the store owner noted down the number of the card, the cheque was guaranteed up to a certain amount. However, due to the introduction of electronic POS terminals and the high cost of processing paper based cheques, the system was abandoned in the 1990s. At the same time, more and more POS payments were made via debit and credit cards.

In 2013, non-cash payments consisted of approximately 6.3 billion credit transfers, 9.9 billion direct debits and 3.7 billion card payments while only 31.2 million payments were made by cheque.

Before the implementation of the Directive 2007/64/EC on payment services in the internal market ("**PSD**"), banks had a monopoly on payment services with the exception of credit card and money transmission business. Leaving aside the special banks, the German banking system is organized in three pillars, consisting of private banks, savings institutions and cooperative banks. Each of these pillars is organized via the respective banking associations which together formed the German Central Credit Committee (Z*entraler Kreditausschuss*; "**ZKA**") which has been renamed DK (*Deutsche Kreditwirtschaft;* "**German Credit Industry**"). Under the auspices of the ZKA, the banking associations, representing their respective member banks have entered into a large number of interbank agreements which form the basis of the German payment systems architecture. Under such system, each bank had a separate bank sort code and via standardized data set, it was possible to clear bank credit transfers on a standardized basis. The German Central Bank ("**Bundesbank**") assisted in the creation of a uniform payment system architecture by providing several different services including a real-time gross settlement system called RTGSplus which was also open towards similar systems in the European Economic Area.

In addition to assuring a common system for credit transfers, the German Credit Industry also has other interbank agreements in place to cover direct debits, ATM payments, POS payments and various other payment-related matters. To the extent it is still relevant, these agreements are listed below under 12.

Besides the regulation of banks as sole parties entitled to render payment services with the exception of card payments and money transmission services, payment services were largely regulated by the general provisions of the German Civil Code (*Bürgerliches Gesetzbuch*; "**BGB**"), the Commercial Code and the general business terms of the banks (which are also largely uniform in Germany).

In 1999, Germany implemented the Directive 97/5/EC on Cross-border Payments and, effective 30 October 2009, Germany implemented the PSD which, among other things also laid the groundwork for SEPA. In particular, as a result of the implementation of the PSD, the monopoly of banks providing payment services was broken by introducing a new type of license for payment services institutions. The regulation of payment services institutions is contained in the German Payment Services Supervision Act (*Zahlungsdiensteaufsichtsgesetz*; "**ZAG**").

Moreover, the implementation of the PSD also significantly changed the private law rules on payment services contained in the BGB. Essentially, Germany implements the PSD without any "gold plating".

2.2 SEPA legal framework

The structures of cashless payments vary from country to country, which often renders cross-border payments cumbersome and slow. In order to make cashless payments simpler, more efficient and more secure across Europe, the Single Euro Payments Area ("**SEPA**") was created in 2008. SEPA offers uniform procedures and standards for transfers and direct debits. The goal is to make payments in euro and across Europe as fast, safe and efficient as national payments are today. SEPA enables customers to make cashless euro payments to anyone located anywhere in Europe, for example by credit transfer, direct debit or debit card. The SEPA project was launched by the European banking and payments industry and is supported by EU governments, the European Commission, the Eurosystem (all national central banks and the European Central Bank ("**ECB**")), and other public authorities. Agreed standards, technical requirements, and a common legal basis are the foundation for payments within the SEPA area, irrespective of the countries involved in the transaction.

After unsuccessful attempts to introduce SEPA via voluntary industry measures, the EU forced the European banking industry into implementing SEPA with the SEPA Regulation No. 924/2009 which was supplemented by the EU Regulation No. 260/2012 which established technical business requirements for credit transfers and direct debits in Euro. In particular, EU Regulation No. 260/2012 provided that by 1 February 2014 credit transfers and direct debits must be carried out in accordance with technical requirements of the regulation. This implies, in particular the use of the BIC and the IBAN as sole permitted identifiers of a payee, thereby abolishing the existing national payment systems architectures including the German system relying on bank sort codes and account numbers. The deadline for expiration of national payment systems was postponed by Regulation No. 248/2014 to 2 August 2014. Moreover, there is a transition period to allow private parties to continue using old account data which the banks will then convert into BIC / IBAN data for purposes of executing payments. The postponement has helped the German banking sector to complete the SEPA transition and has also allowed many companies and smaller associations to change their payment systems interfaces accordingly.

For a more detailed discussion of SEPA, see under 4.2 (d) of the Japanese FSA Research - European Union law aspects.

2.3 Current hybrid status

As a result of the implementation of SEPA, a number of interbank agreements have become obsolete. Most importantly, the interbank agreement regarding credit transfers came out of force on 3 October 2014 and was replaced by a new interbank agreement covering domestic SEPA payments which came into force on 1 February 2014 (see below under 6.12. - SEPA credit transfer agreement). The main obligation under this agreement is to use standardized forms for paper based payments, the obligation to verify the IBAN of the payee before transmitting the payment data and to provide for certain inquiries by the payor's bank to the payee's bank via several institutions to verify whether a payment was received ("chain inquiry"). Otherwise, all other major interbank arrangements that were necessary in order to ensure compatibility of the systems that formed the payment architecture in Germany have been replaced by the relevant provisions of the SEPA rule books issued by the EPC.

The interbank agreement on direct debits (see below under 6.12. - Direct debit transfer agreement) now applies only for direct debits that still follow the own account system for private customers but will cease to be in force by 15 April 2016 when the remaining transition period for private customers has expired.

Again, all necessary interbank arrangements for participation in the direct debit procedure are now part of the SEPA direct debit rule books issued by the EPC (see under 4.2 (f) of the Japanese FSA Research - European Union law aspects). As a result, only the following interbank agreements have remained in place because they are not or not fully affected by SEPA, namely the interbank agreement on the German ATM system (see below under 6.12. - Agreement on the German ATM system), the interbank agreement regarding cashless payments in automatic cash terminals (see below under 6.12. - Agreement on the electronic cash system) and the interbank agreement regarding the prepaid card known as "*GeldKarte*" ("money card") (see below under 6.12. - Agreement on the "GeldKarte" stored value card system).

2.4 Different payment flows in case of credit transfers

The way money flows are settled depends on a number of factors that will determine how a payment is settled.

(a) Accounts of payor and payee with the same institution

This is the simplest form of a money transfer. If payor and payee have an account with the same institution, the institution can simply credit and debit the accounts on the basis of a credit transfer or a direct debit.

(b) Nostro/Loro accounts

If the payor and the payee bank are in a direct business relationship, i.e. one bank maintains an account with the other bank, it will be possible to settle a payments transaction directly between these two banks whereby the bank maintaining the account will refer to the account of the other bank as "loro account" and whereby the bank that is the account holder will refer to that account as so-called "nostro account". A payment is final when the bank which operates the loro account has credited the amount on such account. This type of interbank settlement is no longer very customary in Germany except within banks belonging to the savings and loans group of financial institutions. Also, such settlement method may still be common in case of foreign payments.

(c) Giro networks

In case banks do not maintain accounts with each other, payments transactions will typically be settled via so-called giro networks, more specifically with the "head" institution of such giro network. The most common giro networks are the ones maintained by the savings and loans institutions via their respective top institution in a federal state ("**Landesbank**"). Due to the financial crisis, several Landesbanken had to be closed down or where merged so that some Landesbanken will cover a large number of savings and loans institutions as top institution in a giro network and among the giro networks, clearing is possible via the top institution, namely Deka Bank Deutsche Girozentrale.

In a similar manner, the cooperative banks are organized in giro networks for which two central banks will act as head institutions, DZ Bank and WGZ Bank.

The head institutions will also be able to settle a payment directed to a bank outside of the giro network through appropriate set-off arrangements with the head institutions of another giro network.

(d) Bundesbank services

Moreover, payments can also be settled with the help of the Bundesbank. Bundesbank offers the so-called house bank procedure (*Hausbankverfahren*; "**HBV**"), which consists of three distinct components, HBV-individual, HBV SEPA and HBV IMPay. However, such services are mainly not directed as full service banks but are mainly for (i) payment services providers, (ii) banks which do not have a full bank license (iii) financial services providers (iv) public authorities, (v) private entities who have assumed public tasks or process payments for public authorities as well as (vi) charitable institutions. For these customer groups, Bundesbank maintains accounts just as an ordinary bank and executes payments transactions including both individual payments and so-called "mass payments", particularly international mass payments which are mainly used by public institutions to make payments of pensions or similar recurring payments abroad.

The more relevant service for banks is the TARGET2 payment system described in the next section. Moreover, Bundesbank offers to banks and non-banks the processing of mass payments as a SEPA clearer in the so-called EMZ system. Whenever a payee bank is not a member of the EMZ clearing system, Bundesbank is able to transmit the payment via the system of other clearing infrastructures and also maintains several direct bilateral connections to other European clearing houses, e.g. in Austria, Spain, Netherlands and Bulgaria. The EMZ is mainly designed for payments that do not require immediate execution such as SEPA credit transfers, SEPA core direct debit mandates and SEPA B2B direct debits. Bundesbank can also handle non-SEPA conformant payment formats.

(e) TARGET2

The electronic payment system TARGET2 forms the technical basis for the secure and rapid settlement of cashless payments within the European Union by enabling banks to transfer large amounts in a matter of seconds. Since November 2007, TARGET2 not only allows banks to make payments in real time; it also helps them save liquidity. Additionally, it promotes financial integration in Europe as the system settles not only interbank but also customer payments. TARGET2 is based on a single technical platform and offers all participants services at standardised prices for both domestic and cross-border payment transactions.

TARGET2 is operated by the Eurosystem. TARGET2 is designed for large scale and fast payments. TARGET2 stands for "Trans-European Automated Real-time Gross Settlement Express Transfer System" and allows real-time settlement of payments within seconds. At the moment approximately 350,000 payments with a value of approximately 2.5 trillion Euro are processed on a daily basis. This means that within one year TARGET2 processes approximately 19 million payments with a total aggregated value of 600,000 billion Euro.

Legally speaking TARGET2 consists of a number of national systems which are operated by the relevant central bank but the legal terms of the individual systems are harmonized to a maximum extent. Deviations are only possible under very narrow conditions. The German system has the name TARGET2-Bundesbank ("**TARGET2-BBk**").

It is possible to participate in TARGET2 directly or indirectly. Direct participants require their own RTGS account and access to the information and control module ICM. All regulated banks within the European Economic Area ("**EEA**") are admitted as participants in TARGET2. Indirect participants will clear their TARGET2 payments via a direct participant, i.e. they do not maintain their own RTGS account and can neither deliver nor receive payments directly. Only EEA regulated institutions may act as indirect participants.

One other interesting feature of TARGET2 is that it allows for liquidity pooling by way of a virtual account between several account holders.

Further functionalities include the supervision and management of the minimum reserve requirements and the use of the so-called standing facilities of the ECB, namely the marginal lending facility to obtain overnight liquidity against adjustable assets as well as the deposit facility to make overnight deposits.

2.5 Other forms of payment

(a) Cheque payment

As already discussed, cheque payments do no longer play any commercial importance to Germany. Therefore, we suggest not discussing cheque payments.

(b) Standing Orders

A standing order is a convenient method to instruct a bank to make a recurring payment which is always of the same amount. Therefore, standing orders are used to pay rent or other fixed contributions such as insurance premiums, annuity payments on mortgages and the like.

(c) Direct Debits

Direct debits are so-called "pull" transactions which are initiated by the payee and not the payor. In order to trigger the payment, it is necessary for the payor to have granted a direct debit mandate to the payee.

The SEPA direct debit mandate is slightly different from a legal perspective compared to the prior German direct debit mandate. The prior German direct debit mandate was only an authorization to the payee to directly debit the payor's account, while the SEPA direct debit mandate also includes an instruction from the payor to his bank to make the payment to the payee.

The main function of the direct debit mandate is to allow "pull" payments which can either be recurring or one time payments. Moreover, the recurring payments may be of identical amount or of different amount every month, e.g. a utility bill.

Based on the SEPA direct debit rule books, there are different mandates for payors who are private individuals (SEPA core mandate) and between companies (SEPA B2B mandate). The main difference is that a payment made under a SEPA core direct debit mandate may be revoked by the payor within a period of eight weeks while the SEPA B2B mandate payment cannot be revoked. On the other hand B2B mandates must be confirmed by the payor to his bank before the debit is possible while core mandates do not need any confirmation from the payor given that the payment can be revoked. Of course, none of this prevents a payor from reversing the payment in case he has not validly given the SEPA mandate. Such reversal is possible within a period of 13 months. It should also be noted that before the first direct debit can be effected, the debtor must be notified of the upcoming direct debit, when the direct debit is made for the first time. The pre-notification period is 14 days. However, such period can be shortened by agreement between the payor and the payee.

In the meantime, the volume of direct debit transactions exceeds the volume of credit transfers. Thus, direct debits can be considered the backbone of the German payment systems architecture.

(d) Payments at the POS

(i) normal credit/debit card transactions

Like in any other country, it is possible to pay with credit or debit cards in stores. For that purpose, the card is normally inserted into an electronic terminal which then commences the card authorization process to check whether the credit / debit card limit covers the transaction. The customer will then authorize the payment via PIN or via signature of a paper receipt.

Typically, the merchant will not be in a direct legal relationship with the card issuer but rather have entered into a contract with a merchant acquirer who will process the card transaction for the merchant against payment of a fee. Typically, the acquirer will be able to handle the card transactions of several card brands (VISA, Mastercard, etc.) so that the merchant has only one single point of contact for processing all card transactions effected through the terminal. In some instances, the provision of the technical infrastructure (provision of the terminal, the communications network and the processing of the transactions) may have been outsourced by the acquirer to an acquiring processor who will be acting as a subcontractor of the acquirer. Normally, the acquiring processor will not require a payment services in license for its services but will be able to rely on the exemption for technical services providers (see below under 4.2 - technical service provider exemption). In contrast, acquiring is a licensed activity under the ZAG (see below under 5.).

(ii) electronic cash

As a variant to the above credits / debit card transaction system, the German credit industry operates the electronic cash system which is a standardized system to allow acceptance of giro cards with the electronic cash symbol. Any card issuer who participates in the electronic cash system will guarantee the transactions which its cardholder effects with merchants who also are members of the system.

The system is also linked to the Maestro system of debit cards that is compatible therewith.

Participants in the electronic cash systems benefit from a unified interface and online personalization of security modules. Also the provision of the electronic cash terminals is regulated in the interbank agreement to ensure that the network providers are sufficiently reliable. In addition, this also ensures the compliance with the relevant technical standards. Finally, under the merchant conditions used uniformly with the merchants, the fees for the use of the electronic cash terminals is standardized as 0.2 % of the transaction amount, but no less than Euro 0.04. The electronic cash system interbank agreement also contains a common rule to deal with the losses resulting from the use of forged debit cards.

(iii) retail store cards

Some retail shop operators have also issued store cards which allow the holder of the card to pay by using the card. Essentially, the transactions affected with the store card will be debited from the customer's bank account on a monthly basis. Assuming that the retail store card is issued by the same entity that accepts the card as a means of payment, a retail store card will not require any payment services license.

(iv) closed loop cards

Closed loop cards are cards that have been issued for a limited purpose, usually useable only on specific premises. However, the issuer of the card and the entities accepting the card may not necessarily be the same. Closed loop cards are typically prepaid cards which can be either rechargeable or non-rechargeable. Classical examples of such cards would be cards used in a company cafeteria or so-called "stadium" cards used at a sports venue to pay for relatively small items such as food and drinks. Such closed loop cards essentially avoid the time consuming handling of cash. Closed loop cards are typically exempt from the requirement of a payment services license as explained more fully below under C.2, footnote 1.

(v) direct debit

In order to avoid the fees for card transactions, banks have developed an alternative system under which the debit card would mainly be used to identify the bank account of the customer. The customer would then sign a written direct debit mandate promising also to personally make the payment in case the direct debit is rejected for a lack of funds. The merchant will then simply file the direct debit mandates with his bank and collect the payment from the account of the customer within the normal direct debit mechanism. This type of direct debit exposes the merchant to a considerably higher degree of risk compared to a card transaction both because there is no assurance that the bank account has sufficient coverage and because direct debit payments can be revoked without reason. On the other hand, the system is cheaper than the electronic cash system. However, as a tendency, there is a trend towards greater security, so that the direct debit method has become slightly less popular.

In 2013, transaction volumes with cards could be broken down as follows:

EUR 63.5 billion	direct debit
EUR 144.2 billion	debit cards
EUR 67.5 billion	credit cards

(e) ATM transactions

The main basis for the operation of ATM transactions is the interbank agreement on the German ATM system (*Geldautomaten-System*). The German ATM system is compatible with other international systems such as Maestro and Cirrus based on agreements between the German credit industry and Mastercard worldwide. The interbank agreement will provide for the technical specifications of the card and the ATMs. There is no binding fee agreement except that if the ATM operator charges a fee for the disbursement of cash, such fee must be clearly indicated on the machine. In practice, certain cash groups have been formed which allow withdrawal of cash at the ATM of a respective group member without a fee being charged to the cardholder. The cash groups essentially follow the division of the German banking system into the various pillars (private banks, savings banks and cooperative banks).

(f) Cash payout at the POS

We understand that in Japan it is quite common to disburse cash in small shops who operate a card terminal. This is not a very common form of cash withdrawal in Germany. What is sometimes used is a procedure called "cash-back" when a customer makes a purchase in the supermarket, he may be offered the option to "top up" the card transaction amount and to have the excess amount paid out in cash by the supermarket cashier. The minimum purchase is EUR 20 and the maximum cashback is EUR 200, i.e., the top-up may only be made within the limited range of those two amounts. The cash-back option is part of the electronic cash-system operated by the German Credit Institution. The merchant agrees to the cash payout at the POS in the merchant terms and conditions for participating in electronic cash-system. Among the reasons, why merchants decide to participate in this system is: (i) it reduces the cash holdings of the supermarket and the risk of robberies; (ii) the costs for cash transport and insurance decrease; and (iii) it is a means of customer rentention and customers may buy more to reach the EUR 20 threshold. Participating supermarkets are REWE, Netto-Marken-Discount, familia Handelsmarkt and some EDEKA supermarkets.

In contrast, the fuel stations operating under the Shell brand, in cooperation with Postbank, offer cash withdrawals without a corresponding purchase transaction. Typically, customers will be charged a fee. The maximum amount that can be withdrawn depends on the customer's individual card limits. Another difference is that the fuel stations who offer the service will have a so-called integrated cash management system which means that any money disbursed to the customer will have been checked for forged banknotes.

The Bundesbank recently made a study to determine the motivations of customers using POS cash disbursements. The main reason for using the services is customers who forgot to withdraw cash at an ATM. Generally, most cardholders are not aware of this possibility and use it only as a default option. It remains to be seen whether this cash disbursement method becomes more popular.

(g) E-Money

(i) GeldKarte

The *Geldkarte* is a standardized function associated with the German giro card system. The *GeldKarte* is a chip functionality which allows the customer to load electronic money on the chip of the card. As opposed to debit cards, the payment can normally be made without having to enter a PIN. The *GeldKarte* in feature is not widely used by bank customers but is a practical and convenient way for making micro payments, for example in public transportation or car parks. Sometimes the operators who accept the card will grant a discount for the use of the *GeldKarte*.

The legal basis for the *GeldKarte* system is, again, an interbank agreement which largely defines the technical specifications of the system (see below under 12. - Agreement on the "GeldKarte" stored value card system). It is also possible to unload the card at a cash machine of the issuing bank. If a proper payment transaction has been carried out, the issuing bank will have to guarantee the payments made with the *GeldKarte*. Any amounts payable between banks under the system will be cleared via direct debits.

(ii) Gift cards

Besides the closed loop cards already mentioned above, some retailers also offer gift cards which are essentially prepaid electronic gift certificates that can be used to make a gift to another person that such person can redeem in the participating store. As long as the issuer of the gift card and the entity redeeming the gift card is identical (i.e. the same store chain) the system will not be considered e-money and will therefore not require a payment services license. However, in some circumstances, an e-money license may be required. One example is a franchise system in which the card is issued by another entity than the one operating the individual store. In this case, an e-money license can usually not be avoided unless the so-called "limited network exemption" applies (see below under 4.2). Frequently, the electronic gift card system is managed by an external services provider.

(iii) Mobile payments

Several attempts have been made to establish the mobile phone as a payment device. However, at present, none of these systems have achieved any kind of market significance. The whole area of mobile payments is still very much in flux.

(h) Online payments

Online payments are all payments used in e-commerce situations, in particular in connection with purchases of goods or services on the internet.

(i) debit/credit card payments

Debit/credit card payments operate in the same manner as POS payments except that the customer will usually have to identify himself by some additional security feature instead of PIN or signature. Otherwise the mechanism is identical.

(ii) Prepayment via credit transfer (including Sofortüberweisung)

Many merchants also offer the possibility to prepay the amount. In this case, the merchant will not send the merchandise before the payment has been received on the merchant's account. The customer will use normal means of credit transfers to effect the payment.

As a variation of the above, a service called "Sofortüberweisung" (immediate credit transfer) has been created which essentially creates a connection between the customer and his bank based on the online banking system offered by the individual banks. The operator of the Sofortüberweisung feature offers this "channeling" to allow the customer to immediately instruct a payment with his bank after making an online purchase. After completion of this payment instruction, the customer will be redirected to the website of the online merchant and Sofortüberweisung will confirm to the online merchant that the customer has instructed the payment. Based on the expectation that the instructed payment will arrive, the merchant will then commence the process of delivering the merchandise.

Under the current regulatory regime this type of "channeling" service will not be qualified as payment services and does not require a license. However, the current draft of the second EU Payment Services Directive may submit this type of service to a license requirement (see under 4.2 (b) of the Japanese FSA Research - European Union law aspects).

(iii) SEPA direct debit

Under the current rules of the SEPA rule book, banks are required to agree with their customers that the direct debit mandate must be granted in writing. Therefore, it is strictly speaking not possible to have a payor grant a SEPA direct debit mandate only electronically ("**e-mandate**").

Before the SEPA implementation, there was an understanding in the interbank agreement on direct debits that would allow banks to give their customers permission for electronic direct debit mandates up to a single transaction amount of Euro 50 under certain conditions. It appears as if German banks continue this practice even after the implementation of SEPA. The German SEPA Council, together with the Bundesbank has issued a public statement according to which the implementation of SEPA has not changed anything in the enforceability of electronic direct debit mandates. Nonetheless an online merchant who relies on a purely electronic form of mandate incurs significant risks and may be unable to properly prove that the SEPA direct debit mandate was granted. Therefore, the merchant will face a significant risk that the payment can be reversed for a period of 13 months. This goes significantly above the standard risk that a merchant faces to have a payment revoked within eight weeks without the customer having to give any reason for the revocation. As a result, direct debit mandates are not a common form of online payment.

The EPC has also developed e-mandates in the SEPA direct debit rule books. However, as the German credit industry has pointed out, there is currently no technical infrastructure that would allow the practical implementation of the procedures defined by the EPC.

(iv) E-Money

Many online merchants will accept PayPal payments. PayPal is essentially an e-money issuer that will confirm the payment if the customer has an according balance on his payment account maintained with PayPal. In case of insufficient coverage, PayPal enables the customer to "fill" his PayPal account via a credit card or debit card transaction.

There are also certain providers that offer the purchase of prepaid coupons that can be used to pay for online purchases. The coupons can be purchased in stores and are activated by entering the code printed on the coupon. This type of service is clearly regulated as a payment services under the ZAG.

In contrast, many online providers, e.g. iTunes sell prepaid cards via retailers that can be redeemed for online purchases, but which do not qualify as e-money, because the issuer of the cards is identical to the online provider where the card can be redeemed. Typically such prepaid cards come in standard amounts of 10, 15 or 25 EUR and cannot be reloaded.

(v) Debit via bill of telecommunications carrier

One method of using a mobile device as a means of payment is to debit the amount of the invoice via the bill of the telecommunications carrier. Under normal circumstances, the telecommunications carrier will require a payment services license to provide such service, unless the service that was purchased is also delivered via the device. Therefore, this payment method is limited to payments for online content such as music, videos or games. For more details see below at 4.2 - digital device exemption.

(i) Money transmission services

For the sake of completeness, we also mention the traditional money transmission services operated by Moneygram or Western Union which allow a payor to make a cash payment in one office to have the payment disbursed at another office to a named recipient. Such money transmission services are clearly regulated as a payment services under the ZAG.

(j) Customer loyalty programs (free of charge point services)

It may also be possible to pay for goods and services with "points" and under a customer loyalty program in participating stores. The largest programs are Payback and Miles & More.

The Payback system is operated by an independent operator and allows customers to earn points in participating stores. The points can either be redeemed against premiums which can be directly purchased with Payback or can also be used to make payments or to get cash.

Miles & More is a system operated by a subsidiary of Lufthansa and essentially grants awards in the form of bonus miles on air tickets. It is also possible to earn miles by using the Miles & More credit card which will be issued by a partner bank. Again, the earned miles can be used to purchase airline tickets, upgrade flights or to buy consumer items from the Miles & More website. However, it is also possible to redeem the points in participating stores.

Such loyalty programs are not regulated under the ZAG if certain features are avoided, namely the possibility to purchase additional points against cash and the possibility to transfer points to another customer (for more details see 4.4 below.).

(k) Summary:

Since almost every person in Germany has a bank account, and, as can be seen from the description of the common forms of payment in Germany (2.5), payments services will largely be provided by banks, either directly or indirectly when a payment services provider uses his bank account to transfer received funds to the payee's bank account. The largest number of payments is made by direct debit, followed by credit transfers. The third biggest form of payments is card payments.

3. Overview over payment and settlement related regulations (including matters not relating to laws and regulations)

3.1 Background of Regulation

The current German payment services and e-money law is an implementation of European law and, as such, is part of a larger harmonised legal framework for the creation of an integrated retail payments market throughout Europe. The retail payments market is very dynamic, has experienced a significant innovative pace over the last years and is not confined to national borders. At the same time, payment methods are traditionally different in the European countries with national emphasis on specific payment methods which do not keep pace with the requirements of the market. The PSD, Directive 2009/110/EC on the taking up, pursuit and prudential supervision of the business of electronic money institutions ("**Second E-Money Directive**") and SEPA constitute the current legal framework for a level playing field and ensure accessibility to payments systems for all participants.

3.2 Applicable Regulation

- the ZAG which regulates the rendering of payment services and the using of e-money;
- Sections 675c et seq. BGB which regulate the contractual side of rendering payment services and issuing e-money;
- the Introductory Law to the German Civil Code (*Einführungsgesetz zum Bürgerlichen Gesetzbuch;* "**EGBGB**") which includes information requirements;
- the German Banking Act (*Kreditwesengesetz*; "**KWG**") which, to a limited extent, includes regulations dealing with organizational requirements in case of cashless payment transactions and e-money business, as well as anti-money laundering. The KWG contains European law which is not directly applicable but needs to be implemented into local law, i.e., European directives;
- directly applicable European Regulations (Regulation 1781/2006 on information on the payor accompanying transfers of funds, Regulation 924/2009 on cross-border payments and Regulation 260/2012 establishing technical and business requirements for credit transfers and direct debits in euro) (please refer to 4.2. (d), (e), (h) and (i) of the Japanese FSA Research - European Union law aspects);

- Bundesbank's and German Federal Financial Supervisory Authority's (*Bundesanstalt für Finanzdienstleistungsaufsicht*; "**BaFin**") regulations (including interpretation and guidelines).

4. Payment and settlement services

4.1 Types of regulated payment services in Germany

(a) Payment services

Types of regulated payment services are defined in Sec. 1 (2) ZAG which implements the PSD Annex into German law:

- services enabling cash to be placed on a payment account or enabling cash withdrawals from a payment account, as well as all the operations required in order to operate a payment account ("**deposit and disbursement business**"),
- the execution of payment transactions, including transfers of funds to a payment account with the payment services user's payment services provider or with another payment services provider by:
  - ➢ the execution of direct debits, including one-off direct debits ("**direct debit business**"),
  - ➢ the execution of credit transfers, including standing orders ("**credit transfer business**"),
  - ➢ the execution of payment transactions by means of a payment card or a similar payment instrument ("**payment card business**"),

    without the granting of credit ("**payment business**"),
- the execution of the payment transactions stipulated under number 2 involving the extension of credit **("payment business involving the extension of credit**"),
- issuing payment authentication instruments or accepting and settling payment transactions triggered by payment authentication instruments ("**payment authentication business**"),
- the execution of payment transactions where the consent of the payor to execute a payment transaction is communicated by means of any telecommunication, digital or IT device and the payment is made to the telecommunication, IT system or IT network operator, provided that the operator is acting only as an intermediary between the payment services user and the supplier of the goods or services ("**digitised payment business**"), and
- services where funds are accepted from the payor, <u>without a payment account being created in the name of a payor or a payee</u>, for the sole purpose of transferring a corresponding amount to the payee or to another payment services provider acting on behalf of the payee, or where the amount is received on behalf of and made available to the payee **(**"**money remittance business**").

A **payment account** is an account held in the name of one or several payment services users and serving the execution of payment transactions which shows the accounts receivable and accounts payable between the payment services user and the payment services provider within the business relationship as expressed in the books and for accounting purposes, and determines the payment services user's respective claim on the payment services provider. A payment account is similar to a current bank account which a customer holds with a bank. Both accounts are evidence of the accounts payable and receivable between the account holder and the bank/payment services provider. However, a payment account under ZAG may only be used to perform payment services whereas a bank account may also be used for payments in connection with other banking services provided to the customer. The bank account balance may bear interest and the bank may use the balance for its lending business both of which are characteristic of deposit business which is a banking activity triggering a banking licence requirement. A payment account, on the other hand, may not bear interest and its balance must not be used for the payment provider's other business acitivities but must be separated from its own accounts. In practice, it is sometimes difficult to make the distinction between a current bank account and a payment account. A **direct debit** is a payment transaction initiated by the payee debiting the payor's payment account, in which the payor gives his/her consent to the payee, the payee's payment services provider or the payor's own payment services provider (for more details, see above 2.5.c).

A **payment authentication instrument** is any personalized instrument or procedure that is agreed between the payment services user and the payment services provider for the issue of payment orders and is used by the payment services user to initiate a payment order, i.e. a credit card.

(b) E-money

E-money is not defined as a payment services but on a stand-alone basis. It is defined in Sec. 1a (3) ZAG which implements the Second E-Money Directive into German law as:

Electronic money is defined as all electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of fund for the purpose of making payment transactions and which is <u>accepted by a natural or legal person other than the issuer</u>.

E-money requires a three-sided system, for example the shop operator (for example a franchiser) who accepts a giftcard is not the entity which issues the giftcard (see above under 2. 5 (d) (iii)).

4.2 Exemptions

(a) Payment services

Sec. 1 (10) ZAG contains a list of services that are not considered payment services and corresponds to Article 3 of the PSD:

- payment transactions made exclusively in cash directly from the payor to the payee, without any intermediary intervention,
- payment transactions from the payor to the payee via a commercial agent or central settler authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payor or the payee ("**commercial agent exemption**"),
- professional physical transport of banknotes and coins, including their collection, processing and delivery,
- services where cash is provided by the payee to the payor as part of a payment transaction following an explicit request by the payment services user just before the execution of the payment transaction through a payment for the acquisition of goods or services,
- foreign exchange business settled in notes and coins,
- payment transactions based on any of the following documents drawn on the payment services provider with a view to placing funds at the disposal of the payee:
    - a paper-based cheque within the meaning of the Cheque Act or a similar paper-based cheque under the laws of another Member State of the European Union or another Contracting Party to the Agreement on the European Economic Area,

- a paper-based bill of exchange within the meaning of the Bills of Exchange Act or a similar paper-based bill of exchange under the laws of another Member State of the European Union or another Contracting Party to the Agreement on the European Economic Area,
- a paper-based voucher ("**paper-based voucher exemption**"),
- a paper-based traveller's cheque, or
- a paper-based postal money order as defined by the Universal Postal Union,

- payment transactions carried out within a payment or securities settlement system between settlement agents, central counterparties, clearing houses or central banks and other participants of the system, and payment services providers,
- payment transactions related to securities asset servicing carried out by enterprises falling under the preceding bullet point or by credit institutions, financial services institutions or investment management companies as part of their licence under the KWG or under the Investment Act,
- services provided by **technical service providers**, which support the provision of payment services, without them entering at any time into possession of the funds to be transferred, such as the processing and storage of data, trust and privacy protection services, data and entity authentication, IT and communication network provision, provision and maintenance of terminals and devices used for payment services ("**technical service provider exemption**"),
- services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either for the acquisition within a limited network of service providers or for the acquisition of a limited range of goods or services ("**limited network exemption**")[9],
- payment transactions executed by means of any telecommunication, digital or IT device, if the goods or services are delivered to and are to be used through a telecommunication, digital or IT device, provided that the operator of the telecommunication, digital or IT system or IT network does not act only as an intermediary between the payment services user and the supplier of the goods and services ("**digital device exemption**"),
- payment transactions executed between payment services providers for their own account or between their agents or branches for their own account,
- payment transactions within a group or between members of an undertaking belonging to the same group,
- services by service providers that have not concluded a framework contract with customers, in which funds are withdrawn by means of automated teller machines acting on behalf of one or more card issuers, on condition that these providers do not provide any other payment services, and
- non-professional cash collection and delivery within the framework of a non-profit or charitable activity.

(b) E-money

[9] This exemption is interpreted by BaFin narrowly based on examples provided during the legislative process. As a rule of thumb: the larger the network or the larger the product portfolio that can be purchase the more difficult it is to rely on the exemption. A stadium card (A.5 (d) (iv)) will benefit from the exemption because the use of the card is restricted to the stadium.

The limited network exemption as well as the digital device exemption also apply to e-money.

(c) The commercial agent exemption

To be able to benefit from the commercial agent exemption, the agent must be authorised to negotiate or conclude the sale or purchase of goods or services on behalf of the payor or the payee. He must be involved in the negotiation of the underlying transaction. If he is not involved at all and simply accepts and transfers money, or even if he is involved by transmitting the intention to conclude a contract as a messenger (for example on an intermediary internet platform), the agent cannot benefit from the exemption and performs licensable payment services. For the applicability of the exemption it is not decisive that the payee's right to claim against the payer is extinguished upon the agent's receipt of the payment unless the agent is involved in the conclusion of the underlying transaction.

4.3 Criteria used to categorize a payment and settlement related services to be regulated or to be non-regulated

Whether a payment and settlement related service is regulated or not depends on whether it falls in the defined categories, and if yes, whether exemptions apply. The legislative documents prepared prior to passing the respective implementation acts as well as BaFin guidance provide further clarifications, e.g., by providing examples and limits to the applicability of exemptions.

4.4 Specific questions

Question: The Japanese Payment Services Act does not have the definition of "Funds Transfer Service" (which is defined by case law). Do European countries' regulations have such definition?

Answer: Yes, see above under C.1 which lists the regulated payment services under the ZAG.

Question: How are business activities identified to which payment and settlement regulation apply?

Answer: By analyzing the payment flows und underlying agreements and subsuming under the definitions.

Question: How do European countries regulate payment and settlement services (i.e. what are the criteria by which the regulations applied to payment and settlement services are varied)?

Answer: Differentiating criteria are:

- are payment accounts used?
- pull or push transaction?
- standing order?
- is a payment card used?
- is credit granted?
- is a digital device used

Question: Are the payment and settlement services and deposit are permitted to banks exclusively?

Answer: No, but typically banks will provide payment services. They do not require a separate payment services license.

Question: Do the regulations vary based upon the prepaid payment instrument (ex. prepaid cards), immediate payment instrument (ex. debit cards) and post payment instrument (ex. credit cards)?

Answer: Yes: prepaid cards are subject to e-money regulation. The granting of credit is allowed and if certain conditions are met, the payment services provider does not require an additional banking license (the granting of the credit is carried out as an ancillary activity and is carried out exclusively in the context of the execution of a payment transaction, a term of no longer than 12 months is agreed in the credit agreement and the loan is to be repaid in full within 12 months, and the loan is not extended from the funds received or held for the purpose of executing a payment transaction). Please note that BaFin would not consider card transactions as involving "credit" where the amount is debited to the account of the card holder immediately. Charge cards where amounts are debited to the account at the end of a settlement period will be considered a credit, as well as a revolving credit line combined with the credit card.

Question: Is the free of charge point service regulated? If so how? In addition, do such regulations on free of charge point services vary based upon whether such point can be exchanged with another payment instruments or cash? Is that an area that could be regulated in future, or are you aware of any review or discussion on this?

Answer: Such customer loyalty systems where "points" are earned via purchases of products or services and cannot be purchased against cash payment will not require a payment or services or e-money license if properly structured. In order to avoid the definition of e-money it is critically important to prohibit the purchase of extra points or the transfer of points / miles from one account to another account (i.e., customer transfers points to another customer), because one of the key definitions of e-money is that the e-money is issued against payment of a cash amount. Puchase or sale of points against cash may change the character of the points into e-money. Since in case of transfers between customers, the e-money issuer cannot check whether any consideration is paid, the only solution is to prohibit such transfers completely to avoid the characterization of loayalty points as e-money. Points earned by purchasing airline tickets or other items is nothing but a form of a rebate granted by the participating merchant / airline. Such systems can be operated freely in Germany under the current legal situation.

We are not aware of any discussions or intentions to regulate customer loyalty points systems in Germany.

Question: Under the Japanese Payment Services Act, service providers being registered under the Act are regulated by uniformed regulations, such as assets protection obligations (ex. requirement of cash deposit as performance guarantee, etc.), and regulations on performance/activities (ex. requirement of business structure, information protection system/structure, and information disclosure to clients, etc.). Do the regulations vary based on the services in European countries?

Answer: Yes, regulations vary, too, in particular with respect to initial capital requirements and adequate capital. Otherwise, regulations are similar or identical. To some extent, payment services providers have a certain amount of discretion regarding their business organizations depending on the risk profile of the business. However, compliance with applicable rules will ultimately be reviewed and assessed by the auditors who will submit their report to BaFin.

5. Comparison with Japanese Payment Services

Japan	Germany Please refer to definitions in C.1.a above.
Exchange Transactions by banks or funds transfer service providers	Corresponds to money remittance business assuming the transactions are non-account based. The most known money remittance companies in Germany are Moneygram and Western Union. Essentially the amount is paid in at the payor's location in a local office and a corresponding amount is disbursed at a local office at the payee's

	location which may often be in a different country. The service is popular for persons with a migration background to send money to their family in the home country where the recipient does not have a bank account or to transmit money in emergencies (stolen wallet or similar sudden need of cash). Most money remittance businesses use an agency structure under which independent agents (who may at the same time operate a shop) provide the services under the supervision of the system operator. At the same time, the services have branched out to offer money transmission via the internet. Western Union offers its services in Germany through Western Union Bank, an Austrian Credit Institution operating under a EU passport as regards internet payments and money transmission services offered in own offices, and Western Union Payment Services Ireland Limited (an entity licensed in Ireland and also operating under a EU passport) as regards the services delivered via local German agents. Moneygram delivers its services through Moneygram International Limited, a payment services institution registered with the UK FCA.
Prepaid payment instruments (self-provided or third party-provided; paper-based, IC-based or server-based)	Corresponds to electronic money business. Self-provided instruments where the issuing and accepting party are the same legal person are not regulated. Third party-provided instruments are considered e-money. Paper-based instruments are exempt from regulation, whereas IC-based or server-based instruments fall under the definition of e-money if accepted by another person than the issuer. There are less than ten registered E-money issuers in Germany, which shows that Germany is not the most popular spot for registering such a business in Europe. Most E-money issuers operate based on a license obtained in another EU country (Luxembourg, Belgium and the UK are popular spots) and use the European passport to operate in Germany. The most popular E-money service is *Geldkarte*, ("Money Card") which is an IC-based service usually combined with a debit card and is issued by banks. Its primary purpose is the use in public transport ticket machines, parking facilities to allow very fast payment; for more details, see 2.5.g above. Some credit card issuers (in Germany mostly the banks) also offer credit cards, such as MasterCard to be prepaid (e.g. for minors above 14 years of age

	who cannot yet have a normal credit card or persons with a bad credit history). But this service is used only in such limited circumstances. The biggest player for online prepaid payment solutions is Paypal, a subsidiary of Ebay, Inc. In Europe, Paypal operates via its subsidiary PayPal (Europe) S.à r.l. et Cie, S.C.A, registered in Luxembourg as a bank. It essentially offers payments via prepaid accounts, which, however can be "filled" during payment process via credit card or debit card payment. Paypal has a few competitors such as Click and Buy (#2 in market share, owned by Deutsche Telekom AG and operating based on a UK e-money license). Another player is Amazonpayments (Amazon Payments Europe S.C.A., a payment services provider registered in Luxembourg, but the use of its service is limited to purchases within Amazon (including the web shops hosted with Amazon). Most of the described companies have expanded their service to the offering of so-called digital wallets" which administer several different payment methods, including credit cards, through one electronic bundling feature, specifically to authorize payments made in connection with online purchases. Depending on the mechanism how individual payments are authorized, the operation of such digital wallets may qualify as a payment authentication business and require a payment services license. It is our impression that digital wallets are not yet very popular in Germany. There are numerous offerors of digital wallets in Germany and some of which also offer access via mobile devices. But the market is very fragmented and no really popular service has yet emerged. The same applies for "app" providers who offer payment solutions via mobile phones. May such services are still in the experimental stage. It is possible that in the coming years, mobile phones will become more popular as a payment device if technology is more advanced, e.g. RFID, near-field communication etc. One interesting player for online payments (usually micropayments) is paysafecard, where customers purchase numerical codes (printed on small slips of paper) in small shops or petrol stations which can be redeemed in online stores. Paysafecard is operated by Prepaid Services Company Ltd., which is registered in the UK with the FCA as an e-money issuer and claims to offer the largest prepaid payment solution in Europe with services offered in

	39 countries and accepted in more than 4,000 web shops. It is popular with children who use the e-vouchers to pay for online gaming items, music downloads etc. An example of a gift card issuer operating under an e-money license is Esprit Card Services GmbH, which is one of the few e-money issuers licensed in Germany. They issue an electronic gift card which can be redeemed solely in Esprit retail shops, some of which are operated by franchisees. Due to this acceptance by third parties the gift card meets the definition of e-money. There are numerous smaller card based systems of this type operating under an exemption from the license requirements ("closed loop or limited network exemption) in sports venues to buy food and drinks and souvenir merchandise ("stadium card"). Their primary purpose is to speed up the payment process in order to increase the food and drink sales in periods of high demand (e.g. in the halftime of a game, in-between matches or races etc.) Also, it eliminates the risk of embezzlement by employees. Most visitors will buy the card when they enter the stadium and will redeem any cash left on the card when they leave the stadium (unless they are repeat visitors). Other gift card or similar issuers do not qualify as e-money issuers because they are the only parties who will redeem the card, e.g. Starbucks, which offers the Starbucks Card. In the same category, you will find prepaid cards for mobile phones and web-based stores such as Itunes, Google Playstore and the like. These types of non-reloadable cards are on sale mainly in supermarkets and can be redeemed only with the issuer of the card (MNO, Apple, Google, etc.). Therefore they do not constitute e-money. Paper based systems are not very common in Germany and are typically used in the form of gift certificates. More widely used systems of a national scale are Fleurop (for gifts of flowers) or Bücherscheck for books. Another popular area are meal vouchers handed out to employees (essentially as a replacement to a subsidized employee cafeteria), the most popular is DRS (Deutsche Restaurant Scheck) Because the systems are paper-based, they operate without a payment services license even if the issuer of the voucher is a different person than the merchant who accepts the voucher as means of payment.
Credit card settlements (including issuing,	Issuing credit cards and acquiring business

acquiring and international credit card brand services)	corresponds to payment authentification business. Most credit cards are issued by banks under license agreement by the brands of MasterCard or Visa. American Express is an example of a credit card not issued by a bank, but by the system operator itself. American Express operates based on a European passport and operates a branch office in Germany. Its head office is in the UK where it holds a payment services license from the FCA. Traditionally, genuine "credit cards" in Germany have never been the preferred means of payment and for this reasons, they practically do not exist. Most "credit" cards in Germany are in effect charge cards which are debited once a month from the customer's normal bank account. Credit or charge cards are not liked by merchants because of the high interchange fees. Therefore, debit cards are much more popular in Germany where the transaction amount is debited immediately from the cardholder's account and the fees are lower. Unlike the US, where credit cards are a very popular form of buying goods on credit, German consumers will use an overdraft facility on their giro account to finance their purchases if they are short on money and can basically continue using their debit card until they have "hit" the agreed overdraft limit. Of course, when buying larger items (a car or furniture), consumers will also apply for a normal loan from their bank (at much lower interest rates compared to account overdrafts). One more example of a charge card which does not require a license under the ZAG is a card issued by a department store or retail chain, which allows a customer to buy "on credit". The monthly balance will be debited from the customer's bank account. Popular cards are cards issued by Karstadt (a department store chain) and Breuninger (a chain of clothing stores). As already stated, the vast majority of cards issued by German banks are debit cards under the girocard label which has almost a monopoly in Germany. Every bank in Germany will issue girocards to their account holders and the cards will be used in retail stores and to withdraw cash at ATMs. All ATMs in Germany will accept the girocard, which, in addition is compatible to the Maestro Card (or in some cases vPay) and can thus also be used outside of Germany. Within certain networks, cash withdrawals will be fee of charge. One large network is the cash group, consisting of the largest German private banks (Deutsche Bank, Commerzbank, HVB, Postbank).

	The two other strong networks are of the savings banks and of the cooperative banks. One notable exception is ING Diba, a bank which operates without any branches only via online and telephone banking and which issues VISA cards which can be used to redeem cash free of charge from any ATM with a VISA logo inside and outside of Germany. At the same time parties involved in the execution of payments triggered by a credit card also perform payment card business. There are a number of German acquirers who offer such services (and other related services) to merchants. Large players are b+s Card Service, Concardis, ingenico (formerly easycash), Deutsche Card Services (subsidiary of Deutsche Bank), Payone, Worldpay, Wirecard and Moneybookers (the latter specializing on acquiring of online merchants). Most service providers do not only provide regulated payment services but also related services such as fraud prevention, customer scoring, collection of defaulting debts etc. If the extension of credit is involved, it is payment business involving the extension of credit. As stated above, the linkage between payment service and credit in the form of a genuine "credit" card is not popular in Germany. Credit card brand business, i.e. a credit card organization only provides its logo based on a license agreement with the card issuing bank and sets up the infrastructure and system rules (e.g. Visa, Mastercard) and where credit card agreement is concluded between the card holder and a card issuing bank, is not considered a payment services.
Post-paid type e-money (settlement by credit cards)	Corresponds to the payment business involving the extension of credit. Please refer to C.4. above for a discussion what is regarded as a credit. To our knowledge, post paid type e-money is not in use in Germany.
Payment receiving agency, collection agency	Corresponds to money remittance business assuming the transactions are non-account based. Certain types of collection services, particularly for past due debt or general bill collection may escape regulation, or be subject to different regulation, e.g. factoring business where the payee sells the claim to the factoring company which will collect the claim. Most of such services in Germany operate under a

	different model which does not require a payment services license, for example bill collection services for medical doctors. They prepare the bills for the doctors and send them to the patients and the patients pay the bill to the service company. However, the service company will have purchased the receivable from the doctor (with a discount) and therefore operates under a factoring license. There are numerous such firms operating in Germany.
Account transfer agency	Corresponds to money remittance business assuming the transactions are non-account based. This type of service does not appear to be in use in Germany, because payees will avail themselves of direct debit mandates. The collection of direct debit mandates is traditionally done by the payee's house bank.
Fund transfer agency	Corresponds to money remittance business assuming the transactions are non-account based. This service is not used in Germany. Due to modern online banking systems, mass payments are effected via online data transfers between the payor and his bank and executed via normal credit transfer.
Settlement agency	Corresponds to money remittance business assuming the transactions are non-account based. We assume that such transactions would typically be account based and as such be part of the normal payment services rendered by banks. As explained more fully above (2.4.d), the German Bundesbank also offers this type of services to certain categories of customers.
Cash-on-delivery	Is exempt per explicit statement in draft bill implementing the ZAG. To our knowledge, the only operator of this service ("Nachnahme") is Deutsche Post AG, the formerly state-owned postal service. This service used to be very popular decades ago in the context of mail order business. Since modern mail order business is web-based, most payments in connection with mail orders are nowadays credit card payments, prepayments via credit transfer or online payment services like PayPal that are transacted during the order process. Therefore the "Nachnahme" service is of very limited relevance as a means of payment in Germany.
Escrow services	Depending on the use of a payment account this form of purchaser protection corresponds to payment transaction or money remittance business and is a licensable activity. In Germany, such type of services is typically performed by notaries in real estate transactions (where the use of a notary to

	document the purchase is mandatory). The buyer will typically pay the purchase price to the notary who will put the money on escrow until all payment conditions are fulfilled and it is guaranteed that the buyer will receive free and clear title (through a reservation entry in the land register). The notary then disburses the money and registers the title transfer in the land register. Notaries are exempt from the requirement to obtain a payment services license. In certain complex corporate transactions, banks (their investment banking divisions) are also prepared to accept agency mandates that may involve holding money in escrow. There are certain "trust" services operating to safeguard full delivery of merchandise to customers who pay online merchants. However, to our knowledge this is not done by holding the purchase price in escrow, but rather by some form of guarantee undertaking by the service provider. PayPal offers such a program under the label "purchaser protection" (*Käuferschutz)*. The operation of such service may require a banking or insurance license. One example is Trusted Shops, which does not hold an insurance license but cooperates with insurance companies. Trusted Shops only offers this protection without being involved in the payment flow. If in a "purchaser protection" scheme an internet auction site operator receives money from a winner, keeps it until the auctioned product is delivered to the winner, and then releases the funds to the seller, this would, depending on the use of a payment account, qualify as payment transaction or money remittance business and in both cases require a payment services license.

6. Regulation in Germany

6.1 Licensing scheme, requirements and regulated activities

The ZAG regulates both payment services providers as well as e-money issuers (together "**institutions**"). Providing payment services (please refer to 4.1.a) or rendering e-money business (4.1.b) is subject to a license requirement under the ZAG, if the services or the business are rendered commercially or on a scale which requires a commercially organized business undertaking. Regulation under the ZAG is similar but somewhat less strict than compared to banks.

The ZAG stipulates that CRR credit institutions (banks that are licenced under the KWG (see below under <u>BANKING REGULATIONS AND OTHER - GERMANY)</u> to grant credits and accept deposits) are considered payment services institutions. Therefore, CRR-credit institution can perform payment services but are not required to apply for a separate licence under the ZAG and essentially,for that reason the ZAG does not apply to them at all. They are solely supervised in accordance with and have to comply with KWG rules, including capital requirement rules. Only credit institutions are permitted to engage in deposit-taking activities.

Though an e-money issuer is licenced and supervised under the ZAG, the ZAG stipulates that an e-money issuer is, at the same time, considered a payment services institution. As a result, if the e-money issuer has obtained its licence, the licensee may also render payment services under its e-money license.

Please note that e-money business is stricter regulated than payment services, requiring, in particular with regard to a higher initial capital (EUR 350,000 for e-money or between EUR 20,000 and EUR 125,000 for payment services depending on the specific payment services - see below next paragraph). Capital adequacy rules (see below 6.6 (b) do not necessarily impose higher requirements for e-money issuers but are calculated differently. With regard to separation obligations, the e-money issuer has to comply with specific investment requirments whereas the payment services provider's investment obligations are not clearly defined (see below 6.3 (a)). The reason for differentiating e-money issuers and payment services providers in the ZAG is mainly due to different EU legislative level directives applicable to e-money issuers and payment services providers. The considerable higher initial capital requirement and other additional but more minor differences which an e-money issuer has to be comply with may result from expected higher fund volumes that an e-money issuer handles as a result of e-money being a prepaid product as well as expected higher business operation costs.

The reason for differentiating e-money issuers and payment services providers (both regulated under the ZAG) from banks (regulated under the KWG) is the different treatment on the EU legislative level which was decided to be identically implemented into an act (ZAG) separate from the KWG. The supervision of banks is much more complex and substantially different, in particular with regard to separation rules. Due to the separation rules, customers of e-money issuers and payment services providers enjoy more protection than customer of banks, where no such separations rules exist and customer funds are protected through the general rules which require banks to have sufficient regulatory capital and the deposit protection rules, since in most cases, customer funds will sit in current accounts protected via deposit protection schemes. Under statutory rules, deposits of up to EUR100.000 per customer are protected in case of insolvency of the bank. Finally, e-money issuers and payment services providers are generally considered to be less systemic relevant than banks.

E-money issuers and payment services providers are generally entitled to engage in business activities other than the provision of payment service or e-money. However, BaFin can grant a license on condition that the the other business be split off or that a new company be incorporated for the payment services/e-money acitivities if there is a risk that the other risky business activities may contaminate the financial solidity of the payment institution or the complicate the auditing of the company for regulatory purposes.

(a) License application

The applicant has to comply with the following requirements and has to submit the following documents to the BaFin and the Bundesbank:

- The company needs to have two executive managers (in small companies one executive manager can be sufficient).
- The executive managers must be reliable and have the necessary expertise and experience.
- The owners of the business must be reliable.
- The company must have risk management, internal controls including related to its accounting.
- The company must have its main office in Germany.

- The company must submit an application for the grant of the license with the following content:

    - presentation of its business model: With regard to payment services, the business model has to include a description of the proposed payment services and other activities including a description of how the services will be processed. Draft contracts, including the General Terms and Conditions (*Allgemeine Geschäftsbedingungen;* **AGB**) must be included (Section 2(3) of the ZAG Notification Regulation *(ZAG-Anzeigenverordnung).* With regard to e-money, Section 8a(3) No.1 ZAG includes a similar requirement and demands a description of the proposed issuance of e-money and of the type of the proposed payment services;

    - business plan with a budget forecast for three years and presentation of suitable resources to comply with regulatory requirements;

    - evidence of payment of the initial capital (EUR 350,000 for e-money or between EUR 20,000 and EUR 125,000 for payment services depending on the specific payment services);

    - evidence of the measures taken to separate client monies;

    - description of company management and controls including internal control systems, risk management, accounting procedures;

    - description of the internal controls regarding the prevention of money laundering ("**AML**" or "**ML**") and terrorist finance ("**CTF**" or "**TF**");

    - description of the organizational structure;

    - description of the owners of a significant participation (10% or more) and evidence regarding their reliability;

    - name of the managing directors including evidence regarding liability, expertise and experience;

    - name of the external auditors;

    - legal form and copy of the articles of association; and

    - address of the headquarters or the corporate seat.

- The application must be processed by BaFin within three months from submission of the complete application. This leaves some discretion to the BaFin as to when it deems the submission as complete. Realistically, the preparation and processing of the application will take six to nine months.

(b) Continuing notification requirements

The following continuing notification requirements have to be complied with in accordance with the ZAG Notification Regulation:

- Notify BaFin and Bundesbank without undue delay any significant material or structural change of the actual or legal circumstances which relate to the information and evidence submitted for the license application (see above 6.1.1.).

- Submit financial statements and management report within three months from end of fiscal year to BaFin and Bundesbank (the auditor is obliged to submit the audit report to BaFin an Bundesbank after completion of the audit).
- Notify BaFin and Bundesbank of its intention to perform payment sercices via an agent.
- Notify BaFin and Bundesbank of its intention to outsource material activities and the implementation of the outsourcing.
- Notify BaFin and Bundesbank of its intention to establish a branch in an EEA member state, perform cross-border services into an EEA member state or to to perform payment sercices via an agent in an EEA member state.
- Notify BaFin and Bundesbank of its intention to appoint an executive manager or to appoint a representative with sole representing powers including evidence regarding liability, expertise and experience.
- Notify BaFin and Bundesbank of resignation executive manager or representative with sole representing powers.
- Notify BaFin and Bundesbank of change of corporate form or name.
- Notify BaFin and Bundesbank of the purchase or sale of qualified participating interest in its own institution or the fact that the institution will become a subsidiary of another company, as soon as it becomes aware of the facts.
- Notify BaFin and Bundesbank a loss of 25% of its liable equity capital.
- Notify BaFin and Bundesbank the relocation of its branch or registered seat.
- Notify BaFin and Bundesbank of discontinuation of operations.
- Notify BaFin and Bundesbank the commencement, change or discontinuation of a close link to another natural or legal person (20%).
- Notify BaFin and Bundesbank of its intent to merge with another institution under the ZAG or the KWG.

6.2 Supervisory power of competent authorities

A payment services institution and an e-money institution are supervised by the Bundesbank and the BaFin. Supervisory powers are similar to the powers that can be executed towards banks.

BaFin has the following supervisory powers:

- BaFin may issue orders to institutions and their directors that are appropriate and necessary to stop or prevent violations of regulatory provisions or to prevent or overcome undesirable developments at an institution which could endanger the safety of the assets entrusted to the institution or could impair the proper conduct of the payment services or the proper conduct of the business of e-money issuance.
- Where payment services are provided without a licence or the business of e-money issuance is conducted without the licence, BaFin may order the enterprise as well as its shareholders and the members of its governing bodies to cease business operations immediately and to wind up this business without undue delay. It may issue instructions for the winding-up of the business and appoint a suitable person as the liquidator. The decision will be published on the BaFin website.

- If an enterprise is suspected to provide unauthorised payment services or issue e-money,
  - the members of its governing bodies, the shareholders and the employees of this enterprise shall, on request, provide information about all of the business activities and submit documentation to BaFin and the Bundesbank.
  - BaFin may carry out inspections on the premises of the enterprise as well as on the premises of the persons and enterprises obliged to provide information (see preceding bullet point).
  - The staff of BaFin and the Bundesbank may search the premises of the enterprise and persons and enterprises obliged to provide information (see above). Searches of business premises and persons shall be ordered by a court except in the event of imminent danger.
  - The staff of BaFin and the Bundesbank may seize items which could be of importance as evidence in determining the facts of the case.
- Assess notifications of the acquisition and disposal of qualifying holdings (ownership control procedure, sec. 11 ZAG).
- When evaluating capital adequacy on the basis of an assessment of the business organisation, risk management, loss database and internal control mechanisms as well as the actual risks of the payment institution, BaFin may require the payment institution or the e-money institution to hold an amount of own funds which deviates from the solvency principles by up to 20 per cent.
- During its ongoing business operations, the institution shall, upon request, show and prove to BaFin that it has taken adequate measures to meet the fund separation requirements (see 6.3 below). Where proof is not provided or the measures are not adequate, BaFin may call on the institution to submit the necessary proof or to take the arrangements that are appropriate and necessary to overcome the existing shortcomings.
- Information rights (sec. 14 ZAG)
  - right to request information from institutions, the members of their governing bodies, agents, e-money agents and employees
  - right to conduct onsite inspections (even without a concrete reason)
  - Right to attend shareholder and supervisory board meetings, including the right to speak at such meetings and request to call such meetings.
- Ask for the withdrawal of a senior manager (sec. 15 ZAG).
- In case the own funds requirements are breached, BaFin can order
  - limitations on distributions to shareholders
  - measures to reduce risk.
- Where there is a danger of the discharge of the institution’s obligations towards its creditors, in particular to the safety of the assets entrusted to it, or where there are grounds for suspecting that effective supervision of the institution is not possible, BaFin may take temporary measures to avert this danger. In particular, it may
  - issue instructions to the institution’s management,

- prohibit owners and directors from pursing their business activities or restrict the exercise of these activities,
- appoint supervisors.
- forbid the acceptance of funds and granting of loans,
- issue a ban on sales and payments by the institution,
- order the closure of the institution for business with customers, and
- prohibit the acceptance of payments that are not intended for repaying debts to the institution.

- Lodge a petition for insolvency of the institution.
- BaFin may prohibit the use of agents or e-money agents.
- BaFin may issue orders to an institution that are suitable and necessary for putting into place the arrangements specified in sec. 22 ZAG (see below 6.6).

6.3 Client protection scheme

(a) Description of obligation to keep client funds separate

Under the ZAG, payment services providers (other than banks) and e-money issuers are required to keep all client monies separate from their own funds in a manner such that in an insolvency of the institution, monies are not part of the insolvent estate (Sections 13 (payment services) and 13a (e-money) ZAG). The separation obligation arises if the funds are still held by the payment service provider at the end of the business day following the day when the funds have been received and have not yet beend delivered to the payee or another payment services provider.

As a standard approach, monies need to be deposited in an open trust account at the latest on the day immediately following the date of receipt of such monies (unless such monies have already been paid on to the ultimate payment recipient). An open trust account earmarked as customer funds will be bankruptcy remote, so that customers are protected in case of insolvency of the payment services provider as is required under the ZAG.

Alternatively, it is possible to invest the money in secure low risk liquid assets (normally, money market funds).

As a third alternative, the funds must be covered by an insurance policy or some other comparable guarantee from an insurance undertaking or a credit institution, which does not belong to the same group as the payment institution itself, for an amount equivalent to that which would have to be maintained separately in the absence of the insurance policy or other comparable guarantee and which is payable in the event that the institution is insolvent.

The separation obligations are identical for e-money institutions with the following differences:

The definition of secure assets is slightly different in the case of e-money where the terminology of "secure low-risk assets" is used (omitting "liquid"). For this type of secure low-risk assets, the ZAG explicitly refers to assets falling into a category set out in Table 1 of point 14 of Annex I to Directive 2006/49/EC[10] on the capital adequacy of investment firms and credit institutions for which the specific risk capital charge is no higher than 1.6 per cent, but excluding other qualifying items pursuant to point 15 of that Annex. Further, the ZAG states, that secure low-risk assets within are also units in an undertaking for collective investment in transferable securities (UCITS which are mutual

[10] http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32006L0049&from=EN

funds complying with EU harmonized rules) which invests solely in assets as specified in the first sentence.

In contrast, for payment services providers, the ZAG requires investment in "secure low-risk liquid assets" and leaves it to BaFin to provide a definition which it has not yet provided.

Art. 416 of the Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012 ("CRR") includes a description of liquid assets, inter alia, cash and exposures to central banks to the extent that these exposures can be withdrawn at any time in times of stress; other transferable assets that are of high liquidity and credit quality; transferable assets representing claims on or guaranteed by, inter alia, the central government of a Member State or the central banks and non-central government public sector entities; standby credit facilities granted by central banks within the scope of monetary policy to the extent that these facilities are not collateralised by liquid assets and excluding emergency liquidity assistance. Art 416 CRR, however, does not define what secure low-risk liquid assets are which leaves certain discretion to the payment services provider to chose its investment verhicles to comply with its separation obligations.

The separation obligation arises as soon as the e-money institution receives the funds but at the latest 5 business days after it has issued e-money.

The BaFin ensures proper separation via its right under the ZAG to demand at any time a presentation and evidence that sufficient measures were taken to fulfil the separation obligation. If no evidence is provided, the BaFin can issue an order to produce the documents or to take the necessary measures to ensure separation of the customer fund in line with the legal requirements. If such measures are not taken within the deadline set by the BaFin, the BaFin may take measures such as direct orders to the managers, limit or prohibit the activity of the existing senior managers and owners, and appoint commissioners.

(b) Specific question

How to protect cash held by service providers entrusted by clients? Under the Japanese Payment Services Act, the Exchange Transaction service providers are permitted to conduct its Exchange Transaction amounted only up to 100 million Japanese yen.

Question: Do European countries have such maximum amount on its regulation on the similar service with the exchange transaction?

Answer: In Germany, no such maximum amount rule exists. However, client funds have to be kept separate (see under 6.3.a above). Moreover, there are own funds requirements that are linked to the overall payment volume, described below at 6.6.b.

6.4 Information provision

German law providers for a range of information obligations:

(a) Customer information obligations

Art 248 EGBGB stipulates specific information obligations.

Sec. 2 defines the languages in which information and contract conditions relating to payment services may be drafted (official language from an EEA member state in which the services are offered or the language agreed between the parties).

Secs. 3-12 cover the payment services master agreement (see below under 6.7.a).

Sec. 3 sets forth that information and contract conditions relating to payment services master agreements must be made available in text form on a durable medium.

Sec. 4 contains extensive specific pre-contractual information duties relating to payment services framework contracts, covering

- the payment services provider
- the use of the payment services
- remuneration, interest and exchange rates
- communication
- protective measures and remedies
- amendments and terminations of the payment services master agreement
- venue and choice of law clauses
- the applicable customer complaint procedure under the ZAG and extrajudicial procedure under the Cease and Desist Action Act (*Unterlassungsklagegesetz*).

Sec. 5 obliges the payment services provider to transmit the applicable contract conditions to the customer at his request at any time throughout the duration of the contract.

Pursuant to sec. 6, the payor is entitled to information on the time period required for executing the payment for individual payments as well as on the costs accruing in relation to such payment.

According to sec. 7, the payment services provider is obliged to provide the payor with specific information on the payment once the account of the party making the payment has been charged.

Sec. 8 indicates the information which must be made available to the party making a payment once the payment has been completed.

Under sec. 9 the payment services provider is obliged to notify promptly the payor, if circumstances pursuant to section 4 (1) Nr. 1 change or if interest rate changes to the detriment of the payment services user become effective.

Sec. 10 contains the right to agree on differing rules regarding form and frequency of the information to be provided under sections 7, 8, 9 Nr. 2.

Sec. 11 concerns so-called low-value payment instruments. For such instruments, deviations from sections 675 c ff. BGB regarding providing and using of payment services (cf. section 675 i BGB) may be agreed contractually. Consequently, exemptions from the pre-contractual obligation duties under section 4 apply.

Sec. 12 concerns the formal requirements for single payment agreements not covered by payment services contracts. It is sufficient for such contracts to be easily accessible. The “text form” is unnecessary unless required by the user.

Secs. 13 - 16 cover agreements on single payment transactions.

Sec. 13 enumerates certain information which single payment users must be provided with pre-contractually. Sec. 13 (1) sentence 2 clarifies that the catalogue of sentence 1 is not exhaustive; depending on the circumstances of the case, supplementary information may have to be provided on matters not expressively mentioned in sentence 1.

Sec. 14 lists the information which must be provided to a payor promptly after accessing the payment services order.

Sec. 15, applicable to single payments only, mirrors sec. 8. It contains the minimum information the payment services provider must provide customers with after having executed a payment transaction.

Sec. 16 contains rules regarding comprehensive information duties regarding the payment services provider vis-à-vis the payment services user concerning single payment via a single payment authentication instrument (for the definition of payment authentication instrument please see C.1 above).

Sec. 17 sets forth the information duties applicable to payees made through a single payment authentication instrument.

Pursuant to sec. 18, third parties who are involved in payment transaction must disclose any costs which they may charge users for using specific payment authentication instruments.

Sec. 19 indicates to what extent parties may derogate the requirements under sections 17, 18. Such derogation is only valid where the user is not a consumer.

(b) Distance contracts

If the contract for the provision of payment services is a distance contract, additional information obligations apply. A contract entered into by the payment services provider is considered a distance contract if the other party to the contract is a consumer and the contract is concluded without the simultaneous physical presence of the payment services provider and the consumer, with the exclusive use of one or more means of distance communication up to and including the time at which the contract is concluded. Means of distance communication include phone calls and SMS, Internet websites, ordinary mail, etc. Examples include the online application for a credit card or ordering a prepaid payment instrument by phone.

Pursuant to Article 246b Sec. 1 EGBGB the payment services provider is obligated to provide the other party of a distance contract (i.e. the customer) with the following information:

- if applicable, information about other taxes and/or costs that may exist and are not paid via the payment services provider or imposed by him;
- information regarding any limitations of the period for which the information provided is valid, e.g. regarding the price;
- information regarding the arrangements for payment and performance;
- if applicable, information regarding any specific additional cost for the customer of using the means of distance communication;
- a notice regarding the existence or absence of a right of withdrawal and, where the right of withdrawal exists, its duration and the conditions for exercising it;
- the member states of the European Union whose laws are taken by the payment services provider as a basis for the establishment of relations with the consumer prior to the conclusion of the distance contract; and
- information regarding the existence of guarantee funds or other compensation arrangements, not covered by certain European regulations.

The above-described information must be provided to the customer in a clear and comprehensible manner. The payment services provider could – for example - include the information into the contract form which is provided to the customer by regular mail prior to the conclusion of the contract. Another way would be to provide the customer with the information by e-mail before the customer signs the contract or to have the customer print the information out for signature following online completion of the form.

During the term of the contract the customer may request, at any time, the provision of the terms of the contract (including all applicable standard terms, pricing and any other agreed provision) in printed form (e.g. by regular mail or fax, e-mail is likely to be not sufficient). This right of the customer exists even if the customer has already received a hardcopy of the aforementioned information before entering into the contract.

If the payment services provider does not comply with these information obligations it faces several sanctions, such as cease and desist claims from competitors, fair trading organizations and consumer protection organizations. These claims have been fairly frequent in the past, especially if the information on the withdrawal right was missing or not sufficiently accessible. The provider may also face damage claims, especially from the customers, aimed at the early termination of the contract or the revocation of individual transactions. Also, the period during which the customer may exercise his right to withdraw from the contract may be extended for an unlimited period of time.

(c) E-commerce information obligations

Article 246c Sec. 1 EGBGB stipulates additional information obligations that must be observed by the payment services provider when concluding contracts via E-commerce. E-commerce covers all types of contracts that are concluded via electronic communication and information services, including contracts concluded via the Internet. In such case the payment services provider is obligated to provide the customer with the following information:

- the different technical steps to follow to conclude the contract;
- whether or not the concluded contract will be stored by the service provider after conclusion of the contract and whether it will be accessible to the customer;
- the technical means for identifying and correcting input errors prior to conclusion of the contract;
- the languages offered for conclusion of the contract.
- any relevant codes of conduct to which he subscribes and information on how these codes can be consulted electronically.

If the payment services provider does not comply with these information obligations it may face the same consequences as described above under 6.4.b.

The information obligations for distance contracts and those for E-commerce contracts may apply concurrently, e.g. if a consumer concludes a contract with a payment services provider with the exclusive use of the Internet. However, there are cases where only the distance contract provisions are applicable (e.g. mail orders) and where only the E-commerce provisions are applicable (e.g. conclusion of contracts via the Internet between non-consumers).

(d) Data processing information notices

Pursuant to the Federal Data Protection Act (*Bundesdatenschutzgesetz* - "**BDSG**"), payment services providers (like other data controllers) must provide data subjects (e.g. their customers and any other persons whose personal data they collect, process and/or use) with clear information about the processing of their personal data. The information notice must, for example, describe the identity of the data controller, the kind, extent and purpose of the collection, processing and use of personal data, the categories of recipients, and inform about the processing of personal data outside the EU/EEA (if applicable). Depending on the context in which the personal data is collected, processed and/or used, other notification requirements may apply.

6.5 Data protection provisions

(a) Overview

In Germany, the general provisions on data protection are laid down in the BDSG implementing European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Payment service providers are obligated to observe the general provisions on data protection laid down in the BDSG imposing strict requirements on the collection, processing and/or use of personal data.

If services are provided via electronic communication and information services (e.g. via the Internet) additional sector specific data protection rules apply to such services.

(b) Applicability of the BDSG

The BDSG applies to the collection, processing and/or use of personal data if the data controller:

- is established in Germany and collects, processes and/or uses personal data in Germany; or
- is established in another member state of the European Union ("**EU**") or in another state party to the Agreement on the European Economic Area ("**EEA**"), but collects, processes and/or uses personal data in Germany and such collection, processing and/or use is carried out by a German establishment of the data controller; or
- is established outside the EU/EEA but collects, processes and/or uses personal data in Germany.

This means, that the BDSG is applied according to the principle of territoriality with some exceptions implemented in order to promote the single European market.

Personal data is defined as any information relating to personal or material circumstances of an identified or identifiable natural person (“data subject”). Therefore, the BDSG does not apply to the collection, processing and/or use of information that does not relate and cannot be related to a natural person.

(c) Main principles of German data protection law

- The main principles of German data protection law are:
- direct collection: personal data shall, in general, be collected directly from the data subject;
- data quality: personal data must be accurate and, where necessary, kept up to date;
- data proportionality: personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed;
- transparency: data subjects must be provided with information necessary to ensure fair processing;
- security and confidentiality: technical and organizational security measures that are appropriate to the risks must be taken by the data controller; and
- rights of access, rectification, deletion and objection: data subjects have a right to be provided with the personal information a data controller holds about them and are entitled to have their personal data rectified, amended, or deleted where it is inaccurate or not lawfully processed.

(d) General prohibition of processing personal data

The BDSG prohibits any collection, processing and/or use of personal data unless such acts are expressly permitted or prescribed by a legal provision or if the data subject has validly consented.

The BDSG itself provides for a number of legal permissions that justify a collection, processing and/or use of personal data. For example, such collection, processing and/or use are permitted where they are:

- necessary to create, perform or terminate a legal obligation or quasi-legal obligation with the data subject; or
- necessary to safeguard justified interests of the data controller and there is no reason to assume that the data subject has an overriding legitimate interest in his data being excluded from processing or use.

Moreover, under Sec. 22 (1) sentence 3 No. 4 ZAG, the payment services provider is obligated to have adequate risk-management and adequate control mechanisms, as well as procedures and data processing systems which ensure compliance with the requirements of the Money Laundering Act (Geldwäschegesetz; "**GwG**") and Regulation 1781/2006 (see above under 3.2.) and to investigate dubious or unusual transactions (see also below at 6.10). The payment services provider may collect and use personal data to the extent it has to comply with its obligations under this section. This permission constitutes a legal permission for the processing of personal data and, thus, the payment services provider is not required to obtain the consent of the person whose personal data is collected, processed and/or used for these purposes.

If there is no legal provision permitting or prescribing the collection, processing and/or use of the personal data, such acts require the data subject’s valid consent. Such consent is deemed to be valid only if given voluntarily and on an informed basis. Furthermore, such consent must be given in writing (i.e., by a handwritten signature or by a qualified electronic signature) unless the circumstances allow for a different form.

(e) Data protection authorities

Regarding the private sector there are 17 Data Protection Authorities ("DPA") in Germany in total. One in each of the 16 states (Länder). They all apply the BDSG when dealing with private sector companies. There is also a Data Protection Authority on the Federal level that regularly gives recommendations regarding the interpretation of the BDSG. From state to state funding and staffing of the DPAs differ.

DPAs mainly audit companies and these audits are often launched in reaction to complaints of individuals. Audits usually consist of a request to complete questionnaires but may also include visits on site the companies and interrogations.

(f) Data protection officer

Data controllers are generally obligated to register the collection, processing and/or use of personal data with the competent DPA prior to commencement of such activities. The obligation to register the collection, processing and/or use of personal data does not apply (i) where the data controller has appointed a data protection officer or (ii) where the data controller collects, processes or uses personal data for its own purposes and (a) as a rule, no more than nine staff are permanently deployed for collecting, processing, or using personal data and (b) either the consent of the data subject has been obtained or the collection, processing or use is required to create, carry out, or terminate a legal obligation or a quasi-legal obligation with the data subject.

The aforementioned exception from the registration obligation does, however, not apply in case of automated processing in which the data controller commercially records personal data (i) for the purpose of transfer, (ii) for the purpose of transfer in anonymous form, or (iii) the purposes of market or opinion research.

Payment service providers will most likely be obligated to appoint a data protection officer and, thus, in most cases they will not be obligated to register their collection, processing and/or use of personal data with a DPA.

(g) Possible impact and sanctions

If a data controller violates the BDSG it may be subject to civil and criminal liability (e.g. cease and desist claims, claims for damages and administrative fines).

A data controller may also be obligated to notify the competent DPA and the data subjects if personal data have been unlawfully disclosed to third parties if serious harm to the rights or legitimate interests of the data subjects may occur (security breach notification). This obligation exists only for security breaches with respect to certain types of data categories including personal data concerning bank or credit card accounts.

(h) Data processing activities of payment services providers

The following data processing activities typical for payment services providers are likely to be allowed under the BDSG:

- managing ongoing payment services relationships with the data subject; and
- performing the payment and settlement service including clearance of disputed payments

to the extent the data processing is necessary for these purposes.

The following data processing activities of payment services providers are more difficult to justify:

- direct marketing activities;
- processing personal data for assessing the creditworthiness of a person, using scoring data for this purpose and transferring personal data to rating agencies.

(i) Banking secrecy

Notwithstanding the fact that specific legal provisions on the banking secrecy do not exist in Germany, there is general consent on both term and content of the banking secrecy in legal practice and literature. Such principles have been codified in the General Terms and Conditions of Banks ("*Banken-AGB*") which are almost uniformly used by all German banks. Financial institutions are bound to preserve secrecy on all facts, information, know-how or data on customers relating to the person's data, financial standing, business activities, management, ownership and business relationships as well as the balance and money flows on the account of a customer as well as to his contracts entered into with the payment services provider. The general terms and conditions used by payment services providers typically include provisions concerning banking secrecy.

However, the obligation to observe the banking secrecy does not apply in a number of cases:

- Sec. 11 of the GwG states that payment services providers are obliged to inform the authorities of suspicious cases that may involve money laundering;
- Sec. 93 of the German Tax Code (*Abgabenordnung*) states that everyone (including payment services providers) is obligated to give information as to taxation-related data of their customers; and
- from Sec. 161a in conjunction with Sec. 53 of the German Code of Criminal Procedure (*Strafprozessordnung*) it can be inferred that employees of payment services providers have no right to refuse to give evidence in criminal proceedings.

(j) Information society services

If the payment services is provided via electronic communication and information services the provisions regarding the protection of personal data in the Information Society Services Act (*Telemediengesetz;* - "**TMG**") apply. They must be observed - for example - if services are provided via the Internet (e.g. a website where the customer may download his invoices).

These provisions particularly apply to customer data, i.e. identification information relating to the user of the service and user data, e.g. information regarding start and end of the use of the service and information regarding which services have been requested. Such data may only be collected, processed and or used (i) if necessary for the provision and invoicing of the service; and (ii) for marketing and other limited purposes by creating usage profiles on the basis of pseudonyms unless the user has opted out from creation of such profiles.

6.6 System safety and financial safety management

(a) Technical and organizational safety

The key provision dealing with technical and organizational safety that the institution has to ensure is Sec. 22 ZAG.

Sec. 22 ZAG requires the institution to have a proper business organisation. This includes, *inter alia*, appropriate measures for corporate governance, control mechanisms and procedures to ensure that the institution meets its obligations, the maintaining and updating of a loss database as well as the complete documentation of business activities which ensures full monitoring by BaFin for its area of responsibility, an adequate disaster recovery plan for IT systems, and adequate risk-management and adequate control mechanisms, as well as procedures and data-processing systems to prevent ML and TF.

Corporate governance enables the management to take necessary measures to enable the institution to comply with legal requirements and to ensure the continuance and the development of the institution. To be able to do so in each situation that may arise, the management is obliged to establish a risk controlling and risk reporting system on the basis of the institution's risk profile, i.e., taking into account liquidity risks, operative risks and reputational risks. These, or other relevant materials risks must be monitored and reported.

Control mechanisms include process-related control procedures which require the institution to have organizational guidelines, separation of functions and allocation of competences. Control mechanisms also include process-independent control, which requires an institution to have an internal audit function.

A loss database has to be set-up and maintained. It is a tool to manage operative risks. The loss database documents loss events, such as internal and external fraud, damages which occur in connection with employment practices and workplace safety, damages in connections with clients and products, for example damages resulting from non-compliance with obligations towards a customer, damage to physical assets or in connection with business disruption and system failures or the execution, delivery and process management. The database includes the date and the amount of the incurred damage. The database includes historical data as well as hypothetical future loss scenarios.

Banks are under even stricter organizational requirements under the KWG.

(b) Financial safety

Financial safety is ensured by the separation rules (see above under 6.3). In addition, similar to a bank, an institution has to comply with capital adequacy rules which are defined in more detail in Sec. 13 ZAG (payment services institutions) and Sec. 13a ZAG (e-money institutions) in conjunction with the Capital Adequacy Regulation for Payment Services and E-money Institutions (*ZAG-Instituts-Eigenkapitalverordnung*; "**ZIEV**"). To enable BaFin to monitor compliance with the capital adequacy rules, reports have to be submitted by the institutions on a quarterly basis.

For payment services institutions, the capital requirement is determined by reference to the payment volume processed by the institution. The relevant volume is calculated by reference to the total amount of the executed payment transactions in the preceding year. One twelfth of this amount is relevant for calculating the capital requirement according to a specific calculation method set out in Sec. 4 ZIEV.

The following capital requirements apply under the standard approach ("Method B"):

4 % of the tranche of payment volume up to EUR 5 Million, plus

2.5 % of the tranche of payment volume of more than EUR 5 Million up to EUR 10 Million, plus

1 % of the tranche of payment volume of more than EUR 10 Million up to EUR 100 Million, plus

0.5 % of the tranche of payment volume of more than EUR 100 Million up to EUR 250 Million, plus

0.25 % of the tranche of payment volume of more than EUR 250 Million.

This amount is multiplied with a scaling factor of 0.5 (money transmission), 0.8 (all other cases, except account-based services) or 1.0 for account-based payment services.

Other calculation methods are possible but need to be agreed with BaFin.

For e-money institutions, the capital requirement is determined by reference to the average e-money amount outstanding. The capital requirement is 2 percent of this amount.

Furthermore, institutions have to submit their financial statements to BaFin and Bundesbank. The financials statements as well as compliance with ZAG rules are audited and the auditor's report is sent to BaFin and Bundesbank. The auditor's report serves as an important source of information for the supervisors who will require that non-compliance is remedied. BaFin has also additional intervention powers when capital is insufficient (Sec. 16 ZAG; also see above under 6.2).

(c) Specific questions:

Question: Should a service provider be regulated when individuals take a credit risk of the service providers. Should this be different if business entities (not individuals) take a credit risk of service providers.

Answer: From a German legal point of view, regulation is triggered if a service provider performs payment services. Whether or not the customer (natural or legal person) takes a credit risk, for example, by acquiring e-money, is his/her personal decision. The customers receive protection through the separation rules (see 6.3) and ongoing capital requirements (see 6.6.b.). If the service provider is a bank, protection is afforded through deposit protection schemes and the Basel III-based regulatory capital requirements for banks.

There is no distinction between credit risk protection for consumers or business.

Question: Are there any regulations which ensure the security of payment and settlement system? If you consider that such regulation is necessary, should the regulation be varied based upon the certain criteria?

Answer: There are no specific rules in Germany addressed at payment and settlement systems specifically regarding their security. The systems are operated by payment services providers or banks and thus need to be compliant with system security rules generally applicable to banks and payment services proveiders as described in sec. 8 below. Please refer also to sec. 9 below which covers systemic risk under EU law.

6.7 Description of general civil laws

(a) Payment services agreement and master agreement

Payment services are regulated in Sections 675c – 676c BGB. The provisions on payment services implement the respective provisions of the PSD and to the extent that these provisions do not contain specific obligations, the general law on the execution of transactions on behalf of someone else (*Geschäftsbesorgungsvertrag*) (Sections 663, 665 – 670 and 672 – 674 BGB) shall be applicable (Section 675c (1) BGB). The terminology used in the BGB is identical to the terminology used in the ZAG.

Section 675d BGB specifies that payment services providers have to inform payment services users as further set out in Art. 248 EGBGB (see above under 6.4.a). The information must be provided free-of-charge except where such information is provided more often than legally required, exceeds the framework of Art. 248 EGBGB or is communicated by other means than the ones agreed in the payment services (Section 675d(3) BGB).

A key provision is Section 675f BGB which defines a payment services agreement and a payment services master agreement and also defines a payment transaction. Section 675f(4) BGB specifies that the payment services user must pay the agreed remuneration for the performance of the payment services, but that the performance of ancillary obligations shall only trigger a claim for remuneration unless this is expressly permitted and agreed; moreover, the costs must not exceed the actual costs of the payment services provider.

Section 675f (5) BGB prohibits a provision in the payment services master agreement between a payee and the payment services provider, which excludes the right for the payee to offer a discount for the use of a particular payment-authentication instrument. In other words, a card user may be offered a discount for using a particular payment instrument and the payment services provider must not prohibit such practice. On the other hand, it is clear from this provision that a payment services master agreement which prohibits "surcharging" is allowed. In other words, a payment services provider may prohibit the payee (merchant) from charging an extra fee for the use of a particular payment instrument, e.g. a credit card (to compensate for higher fees payable by the merchant for the use of that card).

Section 675g (1) BGB requires an amendment of a payment services master agreement to be offered with a notice period of two months before the proposed effective date and the payment services provider may agree with the payment services user that the payment services user is deemed to have granted his consent unless he has explicitly rejected the proposed change of the payment services master agreement. In case of rejection of the amendment by the payment user, the payment services provider is entitled to terminate the payment services master agreement. Changes of interest rates or exchange rates shall become effective immediately if such changes are caused by changes of the agreed reference interest rates or reference exchange rates, respectively (Section 675g(3) BGB).

Unless a notice period has been agreed, which may not exceed one month, the payment services master agreement may be terminated at any time by the payment services user, while the payment services provider can only terminate the payment services master agreement if such agreement has been concluded for an indefinite time and a right of termination was agreed. The notice period for termination must not be less than two months (Section 675h BGB).

Section 675i BGB contains a certain relaxation of the rules on payment services agreements for so-called small-amount payment instruments which are instruments for which payment transactions of up to EUR 30 can be initiated with a total expenditure limit of EUR 150 or where the stored value cannot exceed EUR 150 at any time, respectively EUR 200 if the payment instrument is limited to domestic payment transactions.

Another key provision regarding payment services is Section 675j BGB which states that a payment transaction shall only be effective vis-à-vis the payor if the payor has given its consent ("authorization"). The consent can be revoked as long as the payment instruction is revocable in accordance with Section 675p BGB.

Section 675k (2) BGB specifies that the payor and the payment services provider are able to agree that the payment services provider has the right to block a payment instrument in case of security concerns, the suspicion of an unauthorized or fraudulent use of the payment instrument or if, in case of a collective grant of credit, there is a significantly increased risk that the payor is not able to perform its payment obligations. In each case, the payment services provider must inform the payor about the blocking either before or, if this is not possible, immediately after the effectiveness of the blocking. The payment services provider has an obligation to unblock the instrument or replace it if the reasons for the blocking do no longer exist.

Section 675l BGB obligates the payor to take all reasonable precautions to prevent unauthorized access to personalized security features of the payment instruments and must inform the payment services provider immediately of a loss, theft, abusive use or other unauthorized use of the payment instruments after having become aware of it.

Section 675m BGB deals with the effectiveness of a payment instruction, namely it is effective when received by the payment services provider. The payment services provider may reject the instruction but must immediately inform the payment services user (Section 675o(1) BGB). A rejection is not permitted if the instruction satisfies the condition set forth in the payment services master agreement and does not otherwise violate existing legal provisions (Section 675o BGB).

Section 675p BGB deals with the irrevocability of a payment instruction. Normally, the instruction cannot be revoked after having been transmitted or after the payee has received the authorization. A special rule set out in Section 675x BGB applies regarding direct debits (discussed below at 6.7 (d)). A revocation is possible if the payment services user and the payment services provider have agreed on a certain performance date, in which case the instruction can be revoked until the end of the business day before the agreed performance date. A revocation is also possible if explicitly agreed between the payment services user and the payment services provider, but if the payment was already authorized vis-à-vis the payee, then the payee must agree to the revocation of the payment instruction.

Section 675q (1) BGB specifies that the payment services provider of a payor must transmit the full amount and may not deduct the fees from the transmitted amount and Section 675q (2) BGB specifies that the payment services provider of a payee may deduct its remuneration from the transmitted amount only if agreed with the payee.

Section 675s BGB specifies that a payment amount must be received by the payment services provider of the payee at the latest at the end of the day following the date of receipt of a payment instruction. For payment transactions within the EEA which are not conducted in Euro, the payor and the payee may agree on an execution term of not more than four business days. In case of paper-based payment transactions, the term for performance can be extended by one more business day.

Section 675t BGB obligates the payment services provider of the payee to credit the payment amount without undue delay after receipt, i.e. on the same value date.

(b) Distance contracts

Payment service providers must comply with a set of rules concerning conclusion of distance contracts.

These rules implement the European Consumer Rights Directive (2011/83/EU) and the directive concerning the distance marketing of consumer financial services (2002/65/EC) and have mainly been transposed in the BGB and EGBGB. The relevant rules also apply to the rendering of payment services.

In the following, we are outlining some material obligations resulting from such rules (non-exhaustive catalogue):

- Information obligations (see above under 6.4.b)
- Right to withdraw from the contract

  The provisions contain a right of the customer to withdraw from the contract within a period of 14 days without penalty and without giving any reason. The withdrawal period may be extended for an unlimited period of time if the customer has not been properly informed about his right to withdrawal. The EGBGB contains a sample information notice that can be completed and used by businesses to properly inform about the right to withdrawal. In the past, German courts have been very strict regarding the information notice often leading to a possibility of the customer to withdraw from the contract even after the standard withdrawal period has been expired.

  If the payment services is organized by a payment services master agreement between the payment services provider and single contracts that are concluded afterwards on the basis of such payment services master agreement (e.g. the single payment authorizations which may qualify as contracts under German law), the right to withdrawal might only exist with regards to the payment services master agreement.

  In case of a withdrawal, the customer is generally not obligated to perform any payments under the contract and all payments already performed must be reimbursed by the payment services provider. However, the customer is obligated to pay a compensation for those services that have been provided before the withdrawal, if (i) the customer has been duly informed about this obligation prior to the customer placing his binding offer; and (ii) the customer expressly agreed that the performance of the services may begin before the right of withdrawal has expired. The amount payable shall be calculated on the basis of the remuneration for the contract.

- Obligations regarding purchase flows on websites

  The BGB contains specific obligations regarding the design of purchase flows on websites (the provisions apply to all distance contracts concluded via electronic communication and information services, but websites are the most important case).

  - The customer must be provided with technical means to recognize and correct input errors before conclusion of the contract;
  - The customer must be provided with a possibility to access and store the terms and conditions of the contract (including the general terms and conditions);
  - If the contract is concluded by triggering a button and the contract stipulates an obligation of the customer to pay, such button must be clearly labeled with a wording that describes such obligation (e.g. “order with an obligation to pay”); and
  - The customer must be provided with a receipt of the purchase order immediately.

(c) German law on standard business terms

Consumers and other customers of the payment services providers are protected by the strict German law on standard business terms. Standard business terms are all contract terms pre-formulated for multiple contracts which one party to the contract (e.g. a payment services provider) presents to the other party upon entering into the contract. The general terms and conditions of payment services providers will most likely be qualified as standard business terms under the German law on standard business terms.

Standard business terms may be deemed to be unenforceable for numerous reasons (as is often the case). In particular, they may be held unenforceable by a competent court if a clause is considered to constitute an unreasonable disadvantage to the customer or to be not sufficiently transparent. However, the entity having introduced the standard business terms (e.g. a payment services provider) will not be able to claim that a certain clause is unenforceable. Therefore, if a clause provided certain rights to both parties of a contract but is deemed unenforceable, the customer may nevertheless rely on the respective rights while the entity having introduced the standard business terms may not.

If a clause is unenforceable, statutory German law applies instead. In addition, certain organizations (e.g. fair trade organizations or competitors) may raise cease and desist claims against the entity having introduced the standard business terms (e.g. the payment services provider) for the use of unenforceable standard business terms.

The law on standard business terms applies not only vis-à-vis consumers but also in business to business relationships. Although its application is slightly changed to account for market practice, German courts tend to apply strict standards even when reviewing standard business terms that are used in a business to business situation.

German banks use standardized business terms including for payment services rendered by them. These terms have been in use for a long time and have been tested before court. To the extent the specific payment related terms and conditions have been adapted to SEPA recently, their validity may still be disputed.

Payment services providers who are not banks do not use standardized business terms because their business differs depending on the business model. It is more likely that these business terms can and will be successfully disputed before court.

(d) Responsibility in case of fraud/identity theft

In case of an unauthorized payment transaction, the payment services provider of the payor has no claim for costs against the payor and must repay any amounts paid and debited from the payment account (Section 675u BGB).

If a payment instrument has been lost, stolen or has otherwise disappeared, the payment services provider of the payor may claim damages up to an amount of EUR 150. This applies even in case of a fraudulent use of the payment instrument and the payor not having properly safekept the personal security features (PIN, TAN, etc.) (Section 675v(1) BGB).

However, the payor must reimburse the entire damage to the payment services provider resulting from an unauthorized payment transaction if the payor enabled such transaction with fraudulent intent or it was caused by an intentional or grossly negligent violation of its obligations to protect the personalized security features or to notify the payment services provider in case of loss, theft, abusive use or otherwise unauthorized use of the payment instrument.

No liability arises for the payor if he has notified the payment services provider of the loss, theft or abuse of the payment instrument, except where the payor acted with fraudulent intent (Section 675v(3) BGB). In case there is a dispute whether the payment transaction was authorized, the payment services provider must prove due authorization and must further prove that the payment transaction was properly recorded, booked and not impaired by some kind of interference. A payment transaction is considered authenticated if the payment services provider has verified by way of a procedure that the use of a payment instrument included the personalized security features.

A recording of the payment transaction including authentication by the payment services provider does not necessarily suffice to evidence that the payor has authorized the payment transaction, acted in fraudulent intent or violated its obligations (Section 675w BGB).

An important provision for direct debits is Section 675x BGB which states that the payor can revoke a payment transaction initiated by the payee if the authorization did not include the precise amount and the payment amount exceeds the amount that the payor could expect based on its prior expense behavior, the conditions of the payment services master agreement and the circumstances of the individual case. Section 675x(2) BGB specifies that in case of direct debits the payor and the payment services provider may agree that a revocation is possible even without complying with the above-mentioned preconditions. This is the basis on which the EPC has issued the general rule that a SEPA core direct debit mandate entitles the payor to revoke the payment during an eight-week period (see above under A.5.iii). However, it is important to note that the PSD does not mandate such right of revocation in case of direct debits not fulfilling the conditions set out above.

The eight-week period is the maximum time for revocation (Section 675x(4) BGB).

Section 675y BGB deals with the liability of the payment services provider in case of omitted or faulty execution of the payment instruction. No such liability arises if the payment services user has used an incorrect customer ID.

Section 675z BGB limits the liability of the payment services provider to the obligations set out in the statute and for any other liability resulting from a default or faulty performance of a payment instruction can be limited to EUR 12,500. This does not apply for intentional or grossly negligent behavior. The burden of proof whether a payment transaction was properly executed is on the payment services provider (Section 676 BGB). Section 676c BGB contains an exclusion of liability in case of unforeseeable force majeure.

(e) Regulation against fraudulent websites

Question: How can clients be protected from a fraudulent websites? Cases in mind are: scam websites, "phishing" websites, fraudulent telephone calls to ask payment, spoofing and billing fraud.

Answer: Fraudulent websites are not specifically addressed by German law and we are not aware of planned changes to the law in order to address them. However, most fraudulent websites are likely to qualify as fraud under section 263 of the German Criminal Code (*Strafgesetzbuch;* - "**StGB**"). Pursuant to this provision, anyone, who, with the intent of obtaining for himself or a third person an unlawful material benefit, damages the property of another by causing or maintaining a misapprehension by pretending false facts or by distorting or suppressing true facts shall be liable to imprisonment of up to five years or a monetary fine. Victims of such fraud would have a claim for damages against the perpetrators, however, in many cases, the perpetrators operate from foreign countries where judgments from German courts are not enforced or they do not have money to pay compensations.

Claims against the payment services providers are limited: If the client has deliberately authorized the transaction vis-à-vis the payment services provider (e.g. in a “scam website” scheme in the expectation of receiving goods) the general rules applicable for the selected payment method apply (e.g. the right to revoke a payment that has been collected by direct debit, but no right to revoke in case of wire transfer). If the customer did not deliberately authorize the transaction he may have a claim against the payment services provider, depending *inter alia* on his own negligence (see above 6.7.d).

6.8 Regulation relating to technical risk (e.g. prevention/handling of system errors)

(a) MaRisk

The Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement*; "MaRisk") are applicable to banks (please also refer to Research 2 where other aspects of MaRisk are discussed in more detail). Where payment services providers are not banks, MaRisk is not directly applicable because the level of regulation is lower. We can, however, not exclude that external auditors consult the MaRisk as general guidance for their audit also for payment services institutions which are not at the same time banks. With regard to regulation of technical risks, the MaRisk contain some broad requirements regarding the quality and scale of the IT infrastructure. The BaFin has released guidance to further clarify those requirements. They include for example:

- The requirement that the IT infrastructure must safeguard the integrity, availability and authenticity of the data and therefore current technical standards must be observed. Such standards include international norms like ISO/IEC 2700X and standards set out in bulletins released by the German Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnologie – "***BSI***"*). The BSI has released catalogues on basic protection of IT systems (*IT-Grundschutz-Kataloge*) which include catalogues of threats and common safeguards against such threats. The catalogues are available in English language under https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzInternational/itgrundschutzinternational_node.html.

- The requirement to design and grant access rights and roles in IT systems in accordance with the organizational roles of the users of such systems and particularly avoid conflicts of interests and observe separation of roles.

- The requirement to test changes to IT systems before implementing such changes in production environments. Changes must be tested, released and implemented on production systems in a well-defined process and only technically responsible persons may release new or changed IT components.

- The requirement that changes to system parameters may only be made under review of the technical responsible persons and that they have to be release independent from the user.

(b) Technical and organizational measures

The BDSG obligates every entity that collects, processes or uses personal data to take those technical and organizational measures necessary to safeguard that personal data is only processed in compliance with the BDSG. The BDSG contains a non-exclusive list of technical and organizational measures. However, this list is only a very broad description of topics that should be considered.

The list of measures is set out below, together with a short description of each requirement. Moreover, we present some example measures that are not expressly foreseen in the BDSG but which are – in our experience - often taken by businesses in order to comply with the BDSG.

- Access control of processing areas

  Measures to prevent unauthorized persons from having access to the data processing equipment, where the personal data are processed. Measures to comply with this requirement may include:

  - Establishing security areas;
  - Protecting and restricting access paths;
  - Securing the decentralized data processing equipment and personal computers;
  - Establishing access authorizations for employees and third parties, including the respective documentation;
  - Regulations on access cards;
  - Restrictions on access cards;

- All access to the data center where personal data is hosted will be logged, monitored, and tracked;
- The data center where personal data is hosted is secured by an alarm system and other appropriate security measures;
- Access to the building is only granted via a live security guard or via an electronically secured entrance; and
- External visitors are registered at the desk.

- Access control to data processing systems

  Measures preventing that the data processing systems are used by unauthorized persons. Measures to comply with this requirement may include:

  - Automatic time-out of user terminals if left idle, with user identification and password required to reopen;
  - Automatic turn-off of the user identification when several erroneous passwords are entered, along with log file of events (monitoring of break-in-attempts);
  - Encryption methods and requirement regarding identification codes comply with industry standards (minimum length and special characters);
  - Regular password changes;
  - Dedication of individual terminals and/or terminal users, identification characteristics exclusive to specific functions; and
  - All access to data content is logged, monitored, and tracked, in particular information on who edited the content.

- Access control to use specific areas of data processing systems

  Measures ensuring that the persons entitled to use a data processing system are only able to access the data within the scope and to the extent covered by their respective access permission. Measures to comply with this requirement may include:

  - Employee policies and training with respect to each employee's access rights to the personal data;
  - Effective and measured disciplinary action against individuals who access personal data without authorization;
  - Allocation of individual terminals and/or terminal users, and identification characteristics exclusive to specific functions;
  - Monitoring capability with respect to individuals who delete, add, or modify the personal data;
  - Release of data only to authorized persons;
  - Controlled and documented destruction of data;
  - Encryption pursuant to industry standards;
  - Policies controlling the retention of back-up copies; and

- Securing by firewalls.

- Transmission control

  Measures ensuring that personal data during its electronic transmission or during its transport or storage on data storage mediums is prevented from being read, copied, altered or deleted by unauthorized parties, and that it is possible to check and establish to which bodies the transfer of personal data by means of data transmission facilities is envisaged. Measures to comply with this requirement may include:

  - Use of state-of-the-art firewall and encryption technologies to protect the gateways and pipelines through which the data travels;
  - Logging of security violations and regular analysis;
  - Connections to external data processing systems are conducted via encrypted VPN-connection;
  - Encryption complies with industry standards;
  - Due to logging a control of connections is possible afterwards;
  - Data and information will be destroyed by a commissioned document destruction company. Therefore, waste containers for confidential documents are set up; and
  - Avoidance that personal data is stored unencrypted on mobile data carriers and laptops or other mobile devices.

- Input control

  Measures ensuring that it is subsequently possible to check and establish whether and by whom personal data have been input into data processing systems, altered or removed. Measures to comply with this requirement may include:

  - An authorization policy for the input of data into memory, as well as for the reading, alteration, and deletion of stored data;
  - Authentication of authorized personnel;
  - Protective measures for the data input into memory, as well as for the reading, alteration, and deletion of stored data;
  - Utilization of user codes (passwords);
  - Entries to data processing facilities (the rooms housing the computer hardware and related equipment) can be locked; and
  - Automatic log-off of user identifications that have not been used for a substantial period of time.

- Availability control

  Measures ensuring that personal data is protected from accidental destruction or loss. Measures to comply with this requirement may include:

  - Use of back-up and mirroring systems
  - Regular back-up of data

- Server rooms are equipped with effective fire alarms and non-destructive extinguishing systems;
- Infrastructure redundancy;
- Prohibition of the use of private data carriers; and
- All computers are without exceptions equipped with current anti-virus protection.
- Firewalls are checked and updated on a regular basis and protocols are analyzed.

- Separation of Processing for Different Purposes

  Measures ensuring that data collected for different purposes can be processed separately. Measures to comply with this requirement may include:

  - Database separates, which data is used for what purpose, e.g. separation per functionality and function;
  - At the database level, data shall be stored in different normalized tables, and separated per module or function they support; and
  - Interfaces, batch processes, and reports shall be designed for only specific purposes and functions, so that data collected for specific purposes is processed separately.

6.9 Description of regulations relating to systemic risk

On 3 July 2014 the ECB has issued a regulation (Nr. 795/2014) on oversight requirements for systemically important payment systems ("**SIPS**"). A payment system shall be identified as a SIPS if it is eligible to be notified as a system pursuant to Directive 98/26 EC on settlement finality in payment and securities settlement systems by a member state whose currency is the Euro or its operator is established in the Euro area and at least two of the following occur over a calendar year:

- the total daily average volume of Euro-denominated payments exceeds EUR 10 Billion;
- its market chase at least one of the following:
  - 15 % of total volume of Euro-denominated payments,
  - 5 % of total volume of Euro-denominated cross-border payments,
  - 75 % of total volume of Euro-denominated payments as the level of a member state whose currency is the Euro;
- its cross-border activity involves five or more countries and generates a minimum of 33 % of the total volume of Euro-denominated payments processed by that SIPS;
- it is used for the settlement of other financial market infrastructures.

On that basis, the ECB has taken several decisions on 13 August 2014 to determine the following systems as SIPS: TARGET2, EURO1 and STEP2-K as well as CORE(FR).

Article 3 of Regulation 795/2014 specifies that a SIPS operator shall assess whether the applicable law in all relevant legal systems provide a high degree of certainty for and supports each material aspect of the activities of its SIPS and shall establish SIPS rules and procedures and enter into contracts which are clear and consistent with the applicable law in all relevant legal systems and such rules procedures in contracts must be enforceable in all relevant legal systems.

Moreover Article 4 specifies certain governance requirements including objectives which place a high priority on the safety and efficiency of the SIPS which support financial stability and other relevant public interests considerations, in particular open and efficient financial markets. Moreover, a SIPS operator shall have documented governance arrangements and clearly defined board roles and responsibilities. The board composition shall ensure integrity and an appropriate mix of technical skills, knowledge and experience both of the SIPS and of the financial market in general. Also the management roles and responsibilities and reporting lines shall be clearly defined. The board shall establish and oversee a documented risk management framework.

Article 5 provides a framework for a comprehensive risk management.

Article 6 requires the establishment of a robust framework to measure, monitor and manage the credit exposure to its participants and credit exposures amongst participants arising from the SIPS payment, clearing and settlement processes.

Article 7 limits the acceptable collateral for a SIPS operator to cash and assets with low credit liquidity and market risks.

Article 8 requires a SIPS operator to establish a comprehensive framework to manage liquidity risks and must also ensure that if one-sided payments in Euro are settled the participants must hold liquid resources to effect timely settlement of payment obligations in the event of a default of the participant by providing cash or other collateral. The same shall apply for a SIPS operator settling two-sided payments or one-sided payments in currencies other than the Euro. The liquidity risk management measures must also include rigorous stress testing.

Settlement within the system must take place no later than at the end of the intended settlement date (Article 9).

Article 10 requires a SIPS operator to ensure that basically, final settlement must take place in central bank money.

Article 12 of the Regulation requires participant default rules and procedures.

Articles 13, 14 and 15 deal with risk management obligations regarding general business risk, custody and investment risks as well as operational risk.

Article 17 requires the SIPS operator to also monitor indirect participation in the SIPS.

Article 20 also requires a SIPS operator to publically disclose all relevant rules and key procedures.

6.10 Regulation relating to the prevention of money laundering

(a) Overview

Under the GwG, payment services providers as well as e-money institutions are fully caught by AML and CTF obligations which are cumbersome:

(i) Payment services providers as well as e-money institutions have to perform customer due diligence:

- Identify the customer and verify the customer's identity;
- Obtain information on the purpose and nature of the transaction if not self-evident;

- Clarify whether the customer acts for a beneficial owner, identify beneficial owner and verify identity of beneficial owner using risk appropriate measures;
- Ongoing monitoring of the business relationship unless one-off transaction;
- Clarify PEP ("politically exposed person") status of customer and of beneficial owner, and if confirmed, apply appropriate measures to clarify origins of funds;
- Perform additional due diligence measures in specific cases, such as where the client or his/its legal representative is not physically present for the purposes of identification. If not physically present, the transaction payment must be through a payment account in the name of the customer and cannot be made in cash;
- Investigate transactions that are dubious or unusual.
- Due diligence measures must not be repeated if the customer has been identified earlier and data has been recorded, unless there are doubts that the information provided earlier is still correct.
- To a limited extent third party providers can be used for the identification process.

(ii) Enhanced due diligence

Enhanced due diligence obligations according to section 25k KWG apply in case of the settlement of a payment transaction as part of a business relationship with correspondent institutions domiciled in a non-EEA state. The background of this regulation is that payment transactions are settled through the correspondence bank's accounts without knowing the parties behind the transaction. In this case, the German institution has to collect information about the other correspondent institution, must clarify who is responsible with regard to due diligence compliance and must ensure that the correspondent institution does not permit transactions via pass-through accounts. Enhanced due diligence may also be ordered by the BaFin if it becomes aware of substantial risks.

(iii) Simplified due diligence

Simplified due diligence obligations according to section 25i KWG may be applied if the contract complies with certain requirements (in writing, transfer occurs via an account of a credit institution, the transaction is not anonym and cannot be paid out to a third party beneficiary. The transaction amount must not exceed EUR 15,000). However, if the institution suspects ML or TF, simplified due diligence may not be applied.

(iv) Specific regulations for e-money institutions

There are no AML obligations for certain types of e-money below certain threshold volumes (amount must not exceed EUR 100 per month). If the e-money is redeemed into cash upon request of the e-money holder, AML due diligence has to be performed in certain circumstances.

(b) Record keeping

Documents relating to the identity of customers must be retained for 5 years. The retention period starts with the end of the calendar year in which the transaction took place. With regard to passports/identification cards, the nature of the document, number and the issuing agency must be documented; keeping copies or scans of the identification documents is sufficient for record keeping purposes.

(c) Organizational measures and internal control procedures:

Obliged persons are required to put in place internal procedures to assess and manage ML and TF risks. This includes the appointment of an AML officer. The AML officer implements and oversees all actions regarding AML and CTF regulation. He must develop and regularly update an individual AML and CTF combat model for the institution. This contains an analysis of ML and TF hazards as well as the development of work instructions, operating procedures and monitoring systems. The AML officer must report to the management and also is the contact person for BaFin and employees wishing to report suspicious transactions.

(d) Reporting of suspicious transactions

AML rules impose a reporting of suspicious transaction irrelevant of the involved amount.

(e) Audits

The auditor also audits compliance with the GwG and includes any findings in his report which will be submitted to BaFin.

(f) Specific question:

Question: Currently certain service providers not being registered under the Japanese Payment Services Act are not regulated by the money-laundering regulations. How can it be ensured that the money-laundering regulations are applied?

Answer: From a systematic point of view, under German law, application of AML rules for specific parties has to stipulated explicitly in the GwG. Due to the high risk of ML and TF in the payment sector, application of AML and CTF rules has been stipulated in the GwG for all payment services and e-money institutions.

6.11 Application and priority rules in cases where more than one regulation is applicable to such services (including provision of cross border services whether within EU or outside EU)

A credit and deposit taking banking institution licensed under the KWG may provide all payment services regulated in the ZAG without having to obtain a separate ZAG-license. Among the payment services regulated in the ZAG, the issuing of e-money is the highest regulated activity (requiring more initial capital and equity). If an e-money license has been obtained, the e-money issuer may, at the same time, provide all other payment services, without having to obtain a separate license for other payment services.

If not a credit and deposit taking banking institution or e-money issuer, in order to decide which license has to be obtained, it is generally recommended to discuss the business model with BaFin in advance.

Please refer to Research 3 B.2 regarding the different ways of access to the German market, in particular on the basis of the European passport. ZAG contains rules which mirror the KWG rules and allow for a passporting of a payment services license into other European countries.

- An EEA institution has three options: Incorporate a German subsidiary and obtain a German license in the scope required, establish a branch office in Germany based on the rules of the European passport or serve German customers on a cross-border basis without local presence based on the rules of the European passport.
- A non-EEA institution can incorporate a German subsidiary and obtain a German license in the scope required or establish a branch office in Germany (sec. 27 ZAG). As a third alternative, it can incorporate a subsidiary in another EU/EEA country and "passport" the license to Germany under the "European passport" regime. Differently to the KWG, the ZAG does not provide the BaFin with the power to grant exemptions from a license requirement.

If the home supervisor has established that the institution performs a particular payment services, BaFin may not infer with this decision unless it considers that the institution provides services outside of its authorization. Please note that even thought the PSD aims at harmonizing payment services law throughout Europe, we are aware that, in particular, exemptions are interpreted differently in the European countries. If an institution wants to rely on exemptions in another country, it is recommendable to clarify the scope of the exemption with the relevant regulator.

Germany is not a preferred venue for applying for a payment services license or a e-money license, primarily, from our experience, due to the cumbersome AML rules and due to the fact that payment services are primarily rendered through banks. Germany has currently 43 payment services providers and less than 10 e-money institutions.

6.12 Self-regulatory industry rules, voluntary client protection schemes

The German Credit Industry has created the standards in electronic banking which in the form of agreements ("*Abkommen*") are joined by the member banking institutions.

- RDT agreement - includes the EBICS (Electronic Banking Internet Communication Standard) protocoll (*DFÜ Abkommen/Abkommen über die Datenfernübertragung zwischen Kunden und Kreditinstituten*)
- Payment blank form guidelines (Vereinbarung über die Richtlinie für einheitliche Zahlungsverkehrsvordrucke)
- Clearing agreement (Clearingabkommen/ Vereinbarung über den beleglosen Datenaustausch in der zwischenbetrieblichen Abwicklung des Inlandszahlungsverkehrs)
- Online banking agreement - includes the HBCI (Home Banking Computer Interface) protocol, that is now known as FinTS (Financial Transaction Services) (*Homebanking-Abkommen*)
- SEPA credit transfer agreement (Abkommen über die SEPA Inlandslastschrift)
- Direct debit transfer agreement (Lastschriftabkommen/ Abkommen über den Lastschriftverkehr)
- IBAN rules agreement (Abkommen über die IBAN-Regeln)
- Agreement on the maestro debit card safety (*Vereinbarung über die Absicherung der ec-PIN*)
- Agreement on the German ATM system (Vereinbarung über das deutsche Geldautomaten System)
- Agreement on the electronic cash system (electronic-cash-System/ Vereinbarung über ein institutsübergreifendes System zur bargeldlosen Zahlung an automatisierten Kassen)
- Agreement on the "GeldKarte" stored value card system (Vereinbarung über das institutsübergreifende System "GeldKarte")

7. Statistics about payment related services

Please find attached links to studies published by the Bundesbank with statistical information:

- Payment behavior in Germany in 2011 http://www.bundesbank.de/Redaktion/EN/Downloads/Publications/Bulletins_and_surveys/payment_behaviour_in_germany_in_2011.pdf?__blob=publicationFile

- The use of cash and cashless payment instruments http://www.bundesbank.de/Redaktion/EN/Downloads/Publications/Monthly_Report_Articles/2012/2012_10_cash.pdf?__blob=publicationFile
- Statistics on Payments and Securities Trading, Clearing and Settlement in Germany 2009 to 2013 http://www.bundesbank.de/Redaktion/EN/Downloads/Statistics/Money_Capital_Markets/Payment_Systems/zvs_daten_eng.pdf?__blob=publicationFile

BANKING REGULATIONS AND OTHER - GERMANY

1. Glossary

German term	explanation	abbreviation
Landesbank	regional bank	
Pfandbriefbank	covered bonds issuing bank	
Bausparkasse	building society	
Kreditwesengesetz	German Banking Act	KWG
Zahlungsdiensteaufsichtsgesetz	Payment Services Supervision Act	ZAG
Wertpapierhandelsgesetz	Securities Trading Act	WpHG
Bausparkassengesetz	Building Society Act	
Pfandbriefgesetz	Covered Bonds Act	
Finanzkonglomerateaufsichtsgesetz	Financial Conglomerates Supervision Act	FKAG
	Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms and amending Regulation (EU) No 648/2012	CRR
	CRR-institution is an institution within the meaning of Art 4 (1) of the CRR, i.e., an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account	CRR-institution
	European Central Bank	ECB
Liquiditätsverordnung;	Regulation on the liquidity of institutions	LiqV
Großkredit- und Millionenkreditverordnung	Regulation on large loan exposures and million loans	GroMikV
Anzeigenverordnung	Notifications Regulation	AnzV
Solvabilitätsverordnung	Solvency Regulation	SolvV
Bundesanstalt für Finanzdienstleistungsaufsicht	German Federal Financial Supervisory Authority	BaFin
Sparkassengesetze	public savings bank acts	
	European Central Bank	ECB
Deutsche Bundesbank	German Central Bank	Bundesbank
	Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions	SSM Regulation
	risk weighted assets	RWA
Mindestanforderungen an das Risikomanagement	Minimum Requirements for Risk Management	MaRisk
Geldwäschegesetz	German Anti-Money Laundering Act	GWG
Gewerbeamt	local trade office	
	BaFin has established this view in its guidance note 4/2005 for conducting cross-border banking business and/or providing cross-border financial services	BaFin Guidance Note
	European Court of Justice	ECJ
	Anti-Money Laundering	AML
	Counter terrorist finance	CTF

2. Restrictions on the Scope of Business that Banks, Bank Groups, Bank Holding Company Groups, and Financial Holding Company Group may Conduct

Please note that we changed the order of the research because under German and European regulatory law the focus is on the bank itself rather than on the bank group, the bank holding company group or the financial holding company group.

2.1 Restriction on Banks

(a) Overview of the German banking industry

Germany has a universal banking system, i.e., banks, in particular all large banks, provide and are licensed to provide the full range of banking business and financial services. As such, they are also allowed to provide payment services.

German banks can be allocated to one of three groups of banks (German " pillar system") each being represented by an interest group:

- private banks (such as Deutsche Bank, Commerzbank, HypoVereinsbank - see our attached researches)
- cooperative banks with a very local scope. They are assisted by a number of cooperative central banks. After several mergers only two such central banks are left, DZ Bank and WGZ Bank which are essentially owned by the membership institutions (see our attached research for DZ Bank)
- public savings banks (the saving banks are typically co-owners of the regional banks (Landesbanken) together with the federal state(s) in which the Landesbank operates; the regional banks are the central banks of the savings banks and act as the "main bank" of the German federal states) (see our attached research for Helaba).

The fourth pillar is the public bank sector. Public banks are typically held directly or indirectly by the public sector. The Landesbanken (see third bullet point above) also belong to this pillar, as well as public banks acting as business development banks or international project, infrastructure and export financing institutions. A well-known bank in this area is the KfW-Group.

Besides so-called "full banks", which offer the full range of banking services, there are also certain forms of banks with limited business models. Some of which are regulated by special legislation, namely covered bonds issuing banks (*Pfandbriefbanken*) and building societies (*Bausparkassen*).

(b) Definition of a bank

German banking law generally differentiates between two types of regulated entities. First, "credit institutions" which perform banking business, and, second, financial services institutions which render financial services. Both together are referred to as "institution". Another relevant definition is the CRR-institution which is an institution within the meaning of Art 4 (1) of the CRR (see below under A.2), i.e., an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.

German institutions (with one notable exception) do not operate in a holding structure. In almost all cases, a licensed entity is at the top of a group structure and typically holds subsidiaries, which, themselves, can be licensed entities.

There are no particular reasons that could be identified why bank holding company structures are not customary in Germany, but for the fact that Germany has traditionally always had a universal banking system, so that it was always possible to run all banking activities (commercial and investment banking) out of one and the same entity. Typically, bank holding company structures are used to bring together different banking businesses which cannot be performed by the same legal entity. There never was such need in Germany.

Hypo Real Estate Holding was spun off from Hypo Vereinsbank (HVB) in 2003. After bailing out the company, the German government took a 90% stake in Hypo Real Estate Holding in 2009, subsequently squeezed out all remaining shareholders and took the company private. Most problematic assets were transferred to FMS Wertmanagement, a so-called "bad bank", and the two subsidiaries remaining today (Depfa in Ireland and PBB in Germany) are in the process of being either sold or liquidated to comply with EU state aid conditions.

Reasons for establishing a holding were based on the HVB Group's decision as part of a major reorganization plan in autumn 2002 to spin-off its international commerical real estate financing business and its German mortgage banks participation, establishing HRE in 2003 as a specialized commercial real estate finance bank, which was implemented in a few months time in 2003.

Conceptualized as a holding company Hypo Real Estate Holding AG was meant to become a "leading international real estate financing company with European roots, combining commercial real estate financing with modern investment banking", according to Mr. Frank Lamby, Executive Director of the Board of Hypo Real Estate Bank International.

In reality, the holding stucture was probably a product of the special circumstances, namely that Hypo Vereinsbank had bundled several of its commercial mortgage finance operations but failed to merge all of such activities into one single bank entity, presumably for lack of time. At the time of spin-off, Hypo Real Estate held the following bank subsidiaries:

- Hypo Real Estate Bank International, Dublin with its subsidiaries
    - Pfandbriefbank International SA, Luxemburg
    - Certain Real Estate Capital companies in France, Italy, UK and the US
- Württembergische Hypothekenbank-Aktiengesellschaft with subsidiaries; and
- Hypo Real Estate Bank Aktiengesellschaft (itself a product of the merger of three mortgage banks) with subsidiaries (a bank in need of restructuring)

It would probably have been to cumbersome from a regulatory, legal and tax perspective to merge all of these entities or to have one of the bank entities becoming the operating head company of the group prior to the spinoff, particularly in light of the fact that some of the banks were non German.

(c) Applicable regulation

There are various levels of applicable regulations:

- the German Banking Act (Kreditwesengesetz; "KWG") which regulates banks performing banking business and financial services providers rendering financial services. The KWG contains European law which is not directly applicable but needs to be implemented into local law, i.e., European directives;
- the German Payment Services Supervision Act (Zahlungsdiensteaufsichtsgesetz; "ZAG") which regulates the rendering of payment services;
- the German Securities Trading Act (Wertpapierhandelsgesetz; "WpHG") which regulates the rendering of investment services;
- the Building Society Act (Bundessparkassengesetz) which regulates building societies;

- the Mortgage-Covered Bond Act (Pfandbriefgesetz) which regulates banks active in issuance of mortgage-covered bonds.

- directly applicable European law, such as the Regulation 575/2013 on prudential requirements for credit institutions and investment firms ("CRR") with additional technical standards, guidelines and recommendations issued by the European Central Bank (ECB);

- secondary German law enacted by the German ministry of finance, such as the Regulation on the liquidity of institutions (Liquiditätsverordnung; "LiqV"), the Regulation on large loan exposures and million loans (Großkredit- und Millionenkreditverordnung; " GroMikV") and the Notifications Regulation (Anzeigenverordnung; "AnzV") as well as the Solvency Regulation (Solvabilitätsverordnung; "SolvV");

- guidance from the German Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht - "BaFin").

- for public savings banks the public savings bank acts (Sparkassengesetze) of the federal states apply which give the basis for the formation of savings banks as public law entities, their ownership and corporate governance structures.

(d) Supervisory authorities

The European Central Bank ("**ECB**") is the sole regulator of approx. 120 significant Eurozone institutions. In this capacity, the ECB deals has the power to supervise and regulate the following issues:

- Licensing (grant and revocation)
- Significant shareholdings ("ownership control")
- Capital requirements
- Leverage ratio and liquidity requirements
- Governance
- Audits and stress testing
- Consolidated supervision
- Recovery plans, early intervention in case of breach of supervisory requirements.

However, even for these banks, the national regulator remains responsible for the regulation of payment services, consumer protection and AML /CTF.

The ECB has the following powers in its scope of tasks defined in Articles 9 - 18 of Council Regulation (EU) no 1024/2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions ("**SSM Regulation**"):

- All powers of the local supervisor where the ECB replaces the local regulator
- Investigatory powers, namely
  - ➢ the right to request information from credit institutions, financial holding companies, mixed financial holding companies, mixed activity holding companies, all as far as established in the participating member states as well as persons belonging to such entities and those parties to whom tasks were outsourced, and

- the right to conduct investigations, including the right to request the submission of documents, examine the books, obtain written or oral explanations or interview persons
- onsite inspections

- Supervisory powers, namely
    - approve (or reject) draft decisions submitted by the national competent authorities regarding the grant or revocation of a license
    - take decisions on the acquisition of qualifying holdings ("ownership control") based on proposals prepared by the national competent authorities
    - require the supervised institutions to take steps to remedy existing or threatened breaches of the regulatory obligations or to cure organsiational deficiencies, including the right to order institutions to
        - hold more own funds
        - reinforce arrangements, processes, mechanisms and strategies
        - submit a plan to restore compliance with regulations
        - apply specific provisioning policies or treatment of assets for purposes of meeting own funds requirements
        - restrict or limit business, including divestment
        - reduce risk
        - limit variable remuneration
        - use profits to strengthen own funds
        - restrict distributions to shareholders
        - provide additional or more frequent reporting
        - increase liquidity
        - make additional disclosures
        - remove noncomplying members of management
- Right to impose penalties.

For German institutions not being under the sole supervision of ECB, ECB has shared supervisory power with BaFin and the German Central Bank (*Deutsche Bundesbank*; "**Bundesbank"**), The ECB is responsible for

- Licensing (grant and revocation) and
- assessing notifications of the acquisition and disposal of qualifying holdings (ownership control procedure).

The specific scope of tasks shared between ECB and home regulator is defined in the SSM Regulation

The BaFin's powers are defined in the KWG as follows:

- Generally, the BaFin can issue orders to institutions and their senior managers within the scope of its tasks as necessary and suitable to prevent or stop violations of regulatory rules or to stop or remove mischiefs within the institution, which could endanger the security of the assets entrusted to the bank or that impair the proper performance of the institution's bank business or financial services. The BaFin has the same power towards financial holding companies and mixed financial holding companies or persons actually managing the affairs of the institution.

- Grant and revocation of licenses (sec. 32 KWG, unless such power has shifted to the ECB, in which case BaFin is responsible for preparing the decisions). A license can be revoked (sec. 35 KWG), among other things, if

  - the business has not been operated for more than six months
  - a reason is present to have the licenses application rejected
  - there is danger that the institution cannot meet its financial obligations towards third parties
  - the institution has persistently breached its regulatory obligations

- Ask for the withdrawal of a senior manager (sec. 36 KWG)

  - in circumstance that would allow for a revocation of the license or
  - in case the senior manager is not reliable,
  - lacks the necessary skills,
  - does not spend sufficient time to fulfill his tasks or
  - was ignorant of breaches of laws by the institution by reason of failure to exercise proper case and continues such behavior despite a warning by BaFin
  - fails to remedy violations of the regulatory rules despite warning by BaFin
  - (the list is not exhaustive).

- Stop business conducted without the requisite banking or financial services license and order the winding up of the existing business (sec. 37 KWG). For this purpose, BaFin can issue specific orders and also appoint a liquidator.

- Assess notifications of the acquisition and disposal of qualifying holdings (ownership control procedure, sec. 2c KWG), unless such power has shifted to the ECB, in which case BaFin is responsible for preparing the decisions. The main elements can be summarized as follows

  - Any intent to acquire a qualifiying holding (10% or more) or to increase a qualifying holding to 20, 30 or 50% must notify the BaFin in advance
  - The BaFin must decide on such notification within not more than 60 days from submission of complete documents, which can be extendet to up to 90 days
  - The notifier must submit a form and extensive documentation
  - The BaFin can prohibit the acquisition if

- the person is not reliable or for other reasons does not satisfy the requirements for the prudent managment of a bank (which includes the suspicion that the financial means for acquiring the bank stem from criminal activities);
- the bank will not or no longer be able to fulfill its regulatory obligations or the bank would become embedded in a group of enterprise and that due to the complexity of the group structure or lack of economic transparency en effective supervisioj or effective exchange of information is impaired,;
- by acquiring the shares, the bank will become a subsidiary of a foreign financial institution located in a country in which it is not effectively supervised or the regulator is not prepared to cooperate with the BaFin in a satisfactory manner or supervise the bank efficiently;
- the future senior managers are not reliable;
- there is a risk of money laundering or terrorism finance in connection with the planned acquisition or the risk increases by reason of the acquisition; or
- the notifier is not financially sound, which is the case in particular if the capitalization and liquidity of the notifier cannot accommodate the requirements legally imposed on the own funds and liquidity of a bank.

- Information rights (sec. 44 KWG)
  - ➢ right to request information from institutions, the members of their governing bodies and employees
  - ➢ right to conduct onsite inspections (even without a concrete reason)
  - ➢ right to request information from financial holding companies or mixed financial holding companies or members of their governing bodies, including the right of onsite inspections
  - ➢ Right to attend shareholder and supervisory board meetings, including the right to speak at such meetings
- Information rights vis-à-vis holders of a qualifying interest (sec. 44b KWG)
  - ➢ The same rights as specified in sec. 44 also apply towards holds of a qualifying interest, including future holders who have notified their intent to acquire a qualifying participation and persons suspected to hold a qualifying participation
- Right to pursue the conduct of banking business or financial services without license (sec. 44c KWG). This includes
  - ➢ the right of information,
  - ➢ the right to conduct onsite inspections, in cases of urgency also outside normal business hours and the right to perform searches of premises and persons and to seize pieces of evidence
- The right to order improvements of own funds and liquidity (sec. 45 KWG). In particular, BaFin may ask for
  - ➢ submission of a report of past development
  - ➢ measures to better insulate or reduce risk

- measures to increase tier 1 capital, own funds and liquidity
- development of a concept to avoid a potential threat to the ability of an institution to meet its financial obligations

- In case the own funds requirements are breached, BaFin can order
    - limitations on distributions to shareholders
    - prohibit or limit balance sheet measurs to wipe out a loss or show a profit
    - restrict payment on equity instruments from sources other than the profits
    - restrict the grant of loans
    - measures to reduce risk
    - limit or wipe out the available amount for variable compensation of managers and employees
    - order a ban on the payout of variable compensation
    - the submission of a plan to reinstate liquidity
- BaFin take the following measures towards financial holding companies or mixed financial holding companies if such companies fail to comply with their reporting requirements or facts are revealed that demonstrate that the person(s) managing such company is not reliable or lacks the requisite expertise
    - order a ban on the exercise of voting rights
    - order the subordinated companies to not obey to instructions from the holding company if it is not possible to remove the managers of such holding company or attempts to do so have remained futile
    - appointment of a trustee who manages the affairs of the holding company.
- If an institution is not having a proper business organization, BaFin can order
    - measures to reduce risk
    - restrict the opening of further branch offices
    - restrict particular types of business
    - increase of own funds
- BaFin can order the appointment of a commissioner to
    - perform the tasks of senior managers who are not reliable or lack the requisite expertise or if the institution lacks the necessary minimum number of senior managers
    - take measures to restore a proper organization of the business
    - supervise the execution of BaFin orders
    - prepare restructuring plans and supervise their execution
    - review whether claims for damages should be raised against senrio managers or former senior managers who neglected their tasks.

- In emergency situations
    - ➢ give instructions how the institution is managed
    - ➢ prohibit the taking of deposits or the grant of loans
    - ➢ prohibit owners and managers from exercising their functions
    - ➢ issue a preliminary moratorium
    - ➢ close the institution for business with customers
    - ➢ prohibit the acceptance of payments other than to settle a debt owed to the institution
    - ➢ prohibit or restrict
    - ➢ intragroup payments
- Lodge a petition for insolvency of the institution.

(e) Permitted activities

Institutions are permitted to be active within their scope of license (see below under 2.1 (g) (i)). In addition, they may be active where the business activity is explicitly exempt from a license requirement (see below under 2.1 (g) (ii))).

(f) Specific scope of restricted business and restricted activities

(i) Explicitly prohibited activities

The following activities are prohibited according to section 3 KWG:

- the conduct of deposit business if the majority of the depositors are persons employed by the enterprise (employee savings banks), unless other banking business is conducted which exceeds the volume of such deposit business;
- the acceptance of monetary amounts if the majority of the financiers have a legal right to the grant of loans or the procurement of items on credit out of these monetary amounts (special-purpose savings enterprises); this shall not apply to building and loan associations (*Bausparkassen*);
- performing deposit taking or credit taking busisness, if, based on agreement or customary business practices it is excluded or made significantly more difficult to dispose of the credit amount or the deposit amount through cash withdrawal;
- according to Sec. 3 (2) KWG, if certain thresholds are reached, and after a period of twelve months after the threshold has been reached, a CRR-institution or a group which includes a CRR-institution, is prohibited, with certain exceptions, to perform (i) proprietary business; (ii) credit and guarantee business with hedge funds and funds with use leverage to a considerable extent; and (iii) own account dealing. The prohibition is triggered if available-for-sale financial assets or positions "held for sale" or positions allocated to the trading portfolio and liquidity reserves amount to 100 billion Euros or 20 percent of the total assets of the CRR-institution or the group. The balance sheet threshold only applies if the total assets of the CRR-institution or the group were at least 90 billion Euros in each of the last three financial years. The prohibited proprietary trading and related activities have to be split-off into a separate legal entity to ensure, that in case of the insolvency of the separate entity, the risk is isolated from the CRR-institution or the group. The new entity must ensure

its refinancing independently and is subject to terms and conditions applicable to non-group companies;

- building societies are prohibited from offering any other than construction saving plans and certain related business.

(ii) Indirect restrictions

Credit institutions or financial services providers are indirectly restricted from doing business through the following:

- capital adequacy: The purpose of setting aside capital is to enable a bank to absorb losses. The amount of capital that a bank is required to hold, compared to its assets, should be enough to cover unexpected losses and keep it solvent in times of stress. The amount of capital required depends on the kinds of assets that a bank holds - generally, the riskier the asset, the more the capital that has to be set aside. This minimum own funds requirement is expressed as a percentage of its risk weighted assets (**RWA**).

  Essentially banks must cover 8% (currently) of their RWA with own funds. The percentage will increase to 13% until 2019. The risk weight of assets is essentially determined by rating - the safer the asset the lower the risk weight. Internal ratings can be on the basis of a standard model or on the basis of an individual approach.

  If a credit institution's or a financial services provider's equity does not comply with the requirements, it must either refrain from doing certain business or must increase its capital.

  The CRR regulates capital adequacy rules with supplemental rules in the KWG as well as the Solvency Regulation.

- liquidity: Institutions must invest their funds in such a way as to ensure that adequate liquidity for payment purposes is guaranteed at all times. The liquidity risk is the danger that an institution cannot ensure its payment obligations. The liquidity risk is controlled by way of determining and reporting ratios.

  If the liquidity ratios are not complied with, the institution is forced to sell assets.

  The CRR (from 2015/2016 onwards), the KWG as well as the Liquidity Regulation (currently applicable) contain detailed rules to determine the liquidity risk. The liquidity management is part of the institution's risk management for which BaFin provides detailed guidance in its Minimum Requirements for Risk Management (*Mindestanforderungen an das Risikomanagement* - **MaRisk**).

- credit risk: An institution must not incur an exposure to a client or group of connected clients the value of which exceeds 25 % of its eligible capital.

  If a credit has been inadvertently granted, a notification must be made to the regulator. The regulator will determine when and how the credit must be returned.

  The CRR contains detailed rules with regard to large loan exposures, with supplemental rules in the KWG as well as the Regulation on large loan exposures and million loans.

- Loans to corporate officers: the KWG requires that loans to, *inter alia,* members of the management of the institution as well as to family members, to companies in which members of the management of the institution hold an office or to companies holding more than 10% in the institution require specific internal approval of the institution's management and must be at arms's length. BaFin can also determine upper limits for such loans.

(iii) Separation of non-core business

Other than complying with the explicit prohibitions as set out under 5a. and indirect restrictions as set out under 5b. above, a credit institution or financial services provider is generally not prohibited to engage in business that is not his core business. Non-core banking or financial services business is usually performed by subsidiaries, i.e., separate legal entities, with a view to reduce risks for the institution itself and to reduce equity requirements (see below at B.5 for restrictions in operating non-core business via subsidiaries).

Under the ZAG, BaFin can explicitly request that payment services be split-off from the business activities of a company (whether an institution or not) and to incorporate a new company especially for providing payment services. Please also refer to 5.a above regarding splitting-off of proprietary trading business into a separate entity.

(iv) Specific questions

Specific question: Can credit institutions or financial services providers perform identification business, i.e., they provide identification services for companies (individual by using information that the banks have? Identification services provided by IdenTrust (as example) are authentication, encryption, and digital signing.

Answer: Yes, they can. In fact, the institution's identification and verification during its own account opening process can be relied on by other parties who are obliged to identify and verify the identity of a contract partner under the German Anti-Money Laundering Act (*Geldwäschegesetz* - **GWG**). However, in Germany, the post offers standardized identification processes (PostIdent processes with various levels of service (identification in the post office, identification by the postman, etc.)), which is the prevalent service offeror in Germany. Regarding encryption/digital signing these are services typically offered by specialized IT-companies. We cannot exclude that banks hold subsidiaries which offer these products for use in the banking sector.

(g) Requirements for permissions and authorizations

(i) Activities requiring a license

Licensable Activities	
Banking business (Sec. 1 (1) KWG)	Institutions performing banking business are referred to as credit institutions.
1. the acceptance of funds from others as deposits or of other unconditionally repayable funds from the public unless the claim to repayment is securitized in the form of bearer or order notes, irrespective of whether or not interest is paid ;	deposit business
1a. the transactions specified in § 1 para. 1 sentence 2 of the Covered Bonds Act (*Pfandbriefgesetz*);	covered bonds business
2. the granting of money loans and acceptance credits;	lending business
3. the purchase of bills of exchange and cheques ;	discount business
4. the purchase and sale of financial instruments in the institution's own name for the	principal broking business

account of others ;	
5. the safe custody and administrative of securities for others;	security deposit business
6. (deleted);	-
7. the obligation to repurchase previously sold loan receivables prior to their maturity;	repurchase of sold loan receivables
8. the assumption of securities, guarantees and other warranties on behalf of others;	guarantee business
9. the execution of cashless collection of cheques (cheque collection business), collection of bills of exchange (bill of exchange collection business) and the issue of traveller's cheques;	traveller's cheque business
10. the purchase of financial instruments at the own risk for placement in the market or the assumption of equivalent guarantees;	underwriting business
11. (deleted);	-
12. the business of a central counterparty within the meaning of para. 31, which refers Art. 2 of the European No. 648/2012 of 4. July 2012 on OTC derivatives, central counterparties and trade repositories, also known as "EMIR". Under EMIR, certain OTC derivatives require mandatory clearing via central counterparties.	central counterparty
Financial services (Sec. 1 (1) (a) KWG)	Institutions rendering financial services are referred to as financial services institutions.
1. the brokerage of transactions involving the purchase and sale of financial instruments;	investment brokerage
1a. the provision of personal recommendations regarding transactions in specified financial instruments to customers or their representatives, provided that such recommendations are based on a examination of the investor's personal circumstances or presented as being suitable for the investor and are not exclusively announced through information distribution channels or to the public;	investment advice
1b. the operation of a multilateral system which brings together the interests of a large number of persons in the sale and purchase of financial instruments within that system according to specified rules in a way that results in agreements on the purchase of such instruments being entered into;	operation of a multilateral trading facility

1c. the placing of financial instruments without a firm commitment basis;	placement business
2. the sale and purchase of financial instruments in the name of and for the account of others;	contract broking
3. the management of individual portfolios of financial instruments for others on a discretionary basis;	financial portfolio management
4. the continuous offering of financial instruments for purchase or sale on an organized market or on a multilateral trading facility at self-quoted prices, the organized and systematic trading on a frequent basis on an own account basis outside an organized market or a multilateral trading facility by offering a system that is accessible to third parties to conclude transactions with them, the purchase and sale of financial instruments on an own account basis as a service provided to others; the purchase or sale of financial instruments on an own account basis as a direct or indirect participant of a domestic organized market or a multilateral trading facility using a high-frequency algorithmic trading technology characterized by the use of infrastructures aiming at minimizing latency periods, by the decision as to the initiation, generation, passing on or execution of an order being made by the system operating without human intervention for individual transactions or orders, and by a high communication volume throughout the day in the form of orders, quotes or cancellations, also not as a service provided to others .	dealing on own account
5. the brokerage of deposit business with undertakings domiciled outside the European Economic Area;	non-EEA deposit brokerage
6. (deleted);	-
7. dealing in foreign notes and coins;	foreign currency dealing
8. (deleted);	-
9. the continuous purchase of receivables on the basis of framework agreements with or without recourse;	factoring

10. entering into financial lease agreements as lessor and the administration of property companies within the meaning of § 2 para. 6 sentence 1 no. 17;	financial leasing
11. the purchase and sale of financial instruments outside of the management of investment assets within the meaning of § 1 para. 1 of the Capital Investment Code for a syndicate of investors, who are natural persons, with scope of decision making as regards the selection of financial instruments, provided that this is a focal point of the offered product and provided that it serves the purpose of the investors participating in the performance of the purchased financial instruments.	investment management
12. the purchase and sale of securities exclusively for alternative investment funds (AIF) within the meaning of § 1 para 3 of the Capital Investment Code.	restricted custody service business
The purchase and sale of financial instruments on an own-account basis which does not constitute a service for others within the meaning of sentence sec. 1 (1a) sentence 2 no. 4 is also deemed to be a financial service (proprietary business) if the proprietary business is performed by a company that 1. while not being an institution for some other reason, conducts this business commercially or on a scale which requires a commercially organised business undertaking, and 2. belongs to a group of institutions, a financial holding group, a mixed financial holding group or a financial conglomerate that includes a CRR-credit institution.	proprietary business

Financial services institutions may render the following ancillary services without being required to apply for an additional license:

Ancillary investment services, Sec. 2 (3a) WpHG	
1. the safe custody and administration of financial instruments for the account of others and services connected thereto;	safe custody business
2. the granting of credits or loans to others for the carrying out of investment services provided the enterprise granting the credits or	restricted credit business

loans is involved in these transactions;	
3. the provision of advice to companies with respect to the capital structure and the industrial strategy as well as the provision of advice and services relating to the acquisition and mergers of undertakings;	M&A advice
4. foreign exchange transactions which are connected to investment services;	restricted foreign exchange transactions
5. the production, distribution or communication of financial analyses or other information concerning financial instruments or their issuers which directly or indirectly contain a recommendation relating to a specific investment decision;	research business
6. services which are connected to underwriting business;	ancillary underwriting business
7. services relating to an underlying instrument within the meaning of subsection (2) no. 2 or no. 5 and which are connected to investment services or ancillary services.	restricted underlying business

(ii) Activities exempt from a license

Section 2 KWG exempts certain entities from the license requirement e.g. fund managers performing individual portfolio management as an ancillary activity, insurance companies, certain PE companies performing banking business or financial services only within the group (see Research 3 for more detail).

- In addition to the above, a financial services provider is exempt, if
- it administers its own or its affiliated company's employee participation program.
- it acts as a broker or investment adviser of funds registered for distribution in Germany
- professionals, such as lawyers, who render financial service only as an ancillary activity.

Moreover, CRR-institutions do not require a license under the ZAG for rendering payment services (see above under Payment Servise part sec.4.1 (a) with a list of payment services).

(iii) BaFin exemption

Upon application, BaFin can also exempt a company from a certain requirements if the company does not require supervision given the nature of the business which it conducts (Section 2 (4) KWG).

(iv) License application process

The license application needs to be sent to the BaFin and Bundesbank in triplicate. The following documents/information has to be submitted:

- License Application: no form available, letter format, signed by the managing director(s), including: Corporate name, legal form of the entity, registered office (must be in Germany) and address, object of the company, indication which banking business or financial services authorization is being sought, names of the senior managers (generally two, that are reliable and have the necessary professional qualifications), composition of the governing bodies and estimated date on which business operations are likely to commence;

- Constitutive documents;
- Adequate evidence of necessary funds for the business operation (amount depends on type of authorization sought);
- Viable business plan in writing, including, in particular, a description of the nature of the intended banking business with a substantiated indication of its future development, projected balance sheets and projected profit and loss accounts for the first three full financial years after the commencement of business operations, description of the organizational structure of the company, internal control/audit procedures, risk management, documented procedures and policies;
- Detailed ownership control information - if a qualified participating interest in the company is held. Definition of "qualified participating interest": interest that confers, directly or indirectly, at least 10% of the capital of, or the voting rights in the company or if another person can exercise a significant influence on the management of the company;
- Declaration of criminal record to prove trustworthiness of applicant, senior managers and holder of a qualified participating interest;
- Criminal record extract: Provision of a "European Conduct Attestation for Submission to a Governmental Authority" (= Extract from the German criminal record) or equivalent documentation under foreign law in case of foreign nationals for every senior manager of the applicant;
- Curriculum Vitae for every senior manager of the applicant to prove qualification;
- Further Documents if the company is a subsidiary of a foreign entity: If the company is a subsidiary of a foreign credit institution the following further documents are to be submitted: Statement that supervisory authority of parent entity agrees to the incorporation of subsidiary in Germany;
- Additional requirements upon request.

ECB is obliged to grant the license or inform the applicant that the application is denied within six months from having obtained the full set of documents required for the application. BaFin, doing the preparatory work prior to the ECB decision, has a wide scope of discretion to decide whether the set of documents is complete and, thus, can delay the application process. There is not yet any practical experience whether ECB will always follow the BaFin's proposal to grant or deny the license.

BaFin has retained the power to issue and revoke licenses for all banks and financial services providers which do not meet the definition of a CRR credit institution or CRR investment firm. Moreover, BaFin remains the competent regulator to issue payment services licenses under the ZAG,.

An institution must also participate in a public-law investor protection scheme which affords the protection required by the European Deposit Guaranty and Investor Compensation Directives.

As an additional requirement the company needs to register its business with the local trade office (*Gewerbeamt*).

(h) Customer Protection measures (only in respect to non-financial businesses regulations)

Outside the banking and the payment services sector, general customer protection rules apply, such as consumer oriented control of general terms and conditions used by a company, cancellation rights, nullity provisions and information rights. Such measures are discussed in greater detail in Research 1.

2.2 Restriction on Bank Groups, Bank Holding Company Groups, and Financial Holding Company Group

(a) Definition

Various types of groups are defined in the CRR, with the simplest relationship being that of a parent/subsidiary relationship.

A financial holding company is a financial institution, the subsidiaries of which are exclusively or mainly institutions or financial institutions, at least one of such subsidiaries being an institution, and which is not a mixed financial holding company (Art 4 No. 20 CRR).

A mixed financial holding company is a parent undertaking, other than a regulated entity, which, together with its subsidiaries — at least one of which is a regulated entity which has its registered office in the EU — and other entities, constitutes a financial conglomerate (Art 4 No. 21 CRR).

A mixed activity holding company' means a parent undertaking, other than a financial holding company or an institution or a mixed financial holding company, the subsidiaries of which include at least one institution (Art 4 No. 22 CRR).

The CRR further distinguishes between "parent institutions in a member state", being an institution which has further institutions as subsidiaries without itself being a subsidiary of another institution or financial holding company or mixed financial holding company in the same member state (Art. 4 No. 28 CRR) and "EU parent institutions" which is the same and not a subsidiary of another institution, financial holding company or mixed financial holding company in any member state (Art. 4 No. 29 CRR).

The same parallel definitions exist for "parent financial holding company in a member state" / "EU parent financial holding company" and for "parent mixed financial holding company in a member state" / "EU parent mixed financial holding company".

The various types of groups are subject to general and specific rules.

(b) Applicable regulation

The CRR is the most relevant regulation for groups. However it is mainly concerned with prudential consolidation. As a basic rule, the parent institutions in a member state must comply with regulatory capital requirements on a solo basis and on a consolidated basis as well (Art. 11(1) CRR).

As discussed above, in 2.1 (d)., the KWG contains several powers of the competent supervisory authority (BaFin or ECB) to take measures also against financial holding companies and mixed financial holding companies, in particular information rights.

(c) Supervisory authority

Which authority within Europe is responsible to supervise a banking group, financial holding company group or mixed financial holding company group depends on a number of factors.

If the top company in a group is not an institution, then the highest institution in the group (hereinafter the "**consolidating institution**") must meet the regulatory capital requirements on a consolidated basis which includes all subsidiaries of the same parent financial holding company or parent mixed financial holding company (Art. 11(2) and Art. 18 CRR), and if there are several institutions in the same hierarchical level, then the institution with the highest total assets is the consolidating institution (sec. 10a(2) KWG), subject to a diverging determination by the BaFin, e.g. to hold that the financial holding company itself is responsible for the capital consolidation. Morever there are rules which provide that no consolidation of a financial holding group shall take place (in Germany), where there is a financial holding company or a mixed financial holding company in another EU member state which also is a parent of an institution in that member state or there are other institutions in other EU member states and the German financial institution does not have the highest total assets.

In essence this normally leads to capital consolidation taking place at the level of the financial institution at the highest level in the hierarchy with the highest balance sheet total. If this is outside of Germany, then the German authorities are not responsible for supervising the meeting of the capital requirements on a consolidated basis.

Generally, if the bank group, financial holding group or mixed financial holding group includes institutions from several member states, the BaFin must cooperate with the other regulators, in particular in relation to information exchanges (Sec, 8(3) KWG).

Sec. 8a KWG gives BaFin special coordination and information gathering powers to the extent it is the compentent authority for the consolidated supervision, in particular regarding

- coordination of collection and dissemination of information in times of normal supervision and in times of crisis, and
- planning and coordination of supervisory activities in times of normal supervision and in times of crisis.

Moreover, the BaFin will then coordinate the making of a joint decision by all competent regulators for the relevant group whether the own funds of the group on a consolidated basis are sufficient and which additional own funds are required for each single institution and for the group as a whole (sec. 8a (3) KWG. If no joint decision is possible within four months, the BaFin may decide alone whehther the group meets regulatory capital and liquidity requirements on a consolidated basis (sec. 8a (4) KWG). Such decisions shall be taken once a year, subject to updates if needed (sec 8a (5) KWG).

Needless to say that all EU member states have analogous provisions in their local laws to allow for a mirror-image approach in all concerned member states which are based on European law.

Sec. 8d KWG allows BaFin to transfer consolidated supervision of the authority in another member state if supervision by BaFin would be unreasonable and there is another regulator in the EU responsible for consolidated supervision.

Sec. 8e KWG obligates BaFin to set up supervisory colleges for a bank group, financial holding group or mixed financial holding group whenever it is the lead supervisor for consolidated supervision. The EBA defines colleges as "permanent, although flexible, coordination structures that bring together regulatory authorities involved in the supervision of a banking group. In practice, colleges are a mechanism for the exchange of information between home and host authorities, for the planning and performance of key supervisory tasks in a coordinated manner or jointly, including all aspects of ongoing supervision, and also for the preparation for and the handling of emergency situations. One of the fundamental tasks for supervisory authorities as members of colleges is reaching joint decisions on the risk-based capital adequacy of cross-border groups and their EEA subsidiaries." The supervisory colleges serve to exchange information, agree on voluntary assignments of tasks among the regulators, determination of supervisory programmes, removal of unnecessary duplicate requirements, consistent application of supervisory standards and the planning and coordination of supervisory activities in preparation for and in crisis situations (sec. 8e((1) 3rd sentence KWG).

To the extent a financial institution is supervised by the ECB, the ECB will assume the role of the competent regulator in the supervisory college, either as a lead regulator or a normal college member.

(d) Permitted activities

The mere operation of a pure holding company is not a banking or financial services activity that would require any license.

Nor are there any restrictions on the types of companies that can be part of the group.

Each entity in a group of financial institutions is assessed separately on an individual basis whether a and what license is required for its business and will be supervised individually.

(e) Specific scope of restricted business and restricted activities

There is no regulation that would restrict the businesses and activities of bank groups or financial holding groups. The main restrictions come from the prudential rules in the CRR.

- Capital, liquidity (from 2015/2016 onwards), and credit rules must be complied with at the institution's level as well as on the group, i.e., consolidated, level. The CRR provides for waivers that allow for compliance on a group level only in certain circumstances.
- In its Art 89 (with exemption in Art. 91), the CRR contains capital rules for qualifying holdings, the amount of which exceeds 15 % of the eligible capital of the institution (or 60% if the total amount of qualifying holdings is considered) in an undertaking which is not
  - (i) a financial sector entity;
  - (ii) an undertaking, that is not a financial sector entity, carrying on activities which the competent authority considers to be any of the following:
    - a direct extension of banking;
    - ancillary to banking;
    - leasing, factoring, the management of unit trusts, the management of data processing services or any other similar.

For such holdings prohibitively high capital rules apply which basically results in a restriction to hold such companies, because according to Art. 89 (3) CRR a risk weight of 1250% must be applied, which effectively means that such acitivies will be fully deducted from the bank's available own funds. Details will be clarified in guidelines to be issued by EBA.

- If a group also includes an insurance company and exceeds certain thresholds, it is subject to the financial conglomerate supervision with additional restrictions. Transactions within the conglomerate may not exceed certain thresholds and must comply with certain restrictions.

  This regulation with respect to Financial conglomerates is set out in the Financial Conglomerates Supervision Act (*Finanzkonglomerateaufsichtsgesetz*; "**FKAG**") which implements the relevant EU Directive (No. 2011/89/EC of 16 November 2011) which has amended the original EU Directive on Financial Conglomerates of 2002.

  Financial conglomerates are defined as groups which consist of at least one company from the banking or investment services sector and at least one company from the insurance sector. If the top company in the group is not a supervised entity, the definition is only met if the group acts predominantly n the financial sector (at least 40% of total assets). A separate supervisory regime for financial conglomerates applies only where certain relevancy thresholds defined in sec. 8 FKAG are exceeded (each separate sector activity accounting for at least 10% of a group's activities with the smallest sector accounting for at least 6 billion EUR in total assets). Banking and investment activities are counted together for this purpose.

  The key elements of regulation are sec. 17 and 18 FKAG, which provide that financial conglomerates must meet own funds requirements on a consolidated basis and how these are calculated. If the BaFin is the competent regulator, it has substantial supervisory powers to take measures to ensure compliance with the requirements.

The compliance with such own funds requirements will be cumulative to the own funds requirements applicable to the individual banks or other members of the financial conglomerate.

Transactions within the conglomerate require a unanimous resolution of the governing bodies of the relevant group companies and the supreme company is responsible to ensure there is no significant concentration of risk resulting from such intragroup transactions. Risk concentrations must be notified to BaFin (sec. 23 FKAG)

Because the regime under the FKAG only concerns mixed groups and addresses the specific risks of cross-sector activities, this regulation on a consolidated basis is beyond the scope of our discussion. We will therefore not elaborate on the details of the regulation of financial conglomerates. To our knowledge, there are only seven financial conglomerates in Germany (source: statement by Bundesbank of 10 April 2013 in a public hearing when draft FKAG was discussed) , most of which are headed by insurance companies. For more detail, see also the EU law part of this memo at section 4.2 (h).

- According to Sec. 13c KWG, if a CRR-institution belongs to a mixed group, certain group internal transactions exceeding certain thresholds (still to be defined by a regulation) must be notified to BaFin and is subject the BaFin's consent. In the absence of a regulation Sec. 64g KWG stipulates the following group transactions as reportable: loans, sureties, guarantees and other off balance sheet transactions, specific insurance related transactions, capital investment, reinsurance transactions and cost allocation agreements. Such a transaction is relevant if the individual transaction reaches or exceeds 5 percent of the capital requirements on the group level. Various transactions with the same group company need to be combined to calculate the threshold.

(f) Permissions and authorizations

The group itself is not subject to an authorization or license requirement. Nor is the operation of a financial holding company as such subject to a license requirement. Each group company must meet applicable license requirements for the type of business it operates.

If a group is formed which includes institutions, typically, the ownership control procedure (sec. 2c KWG) will have to be complied with, since the formation of a group (or the addition of a new institution to the group by way of acquisition or merger) will involve the acquisition of a qualifying interest in such institution. The BaFin or the ECB, as the case may be, can prohibit the transaction, among other reasons, if the acquired institution would not be able to comply with its regulatory obligations as a result of the acquisition or if the institution would be embedded in the group in a manner that makes supervision difficult due to the intermingled structure of the participation or because of lack of transparency (sec. 2c(1b) no. 2 KWG). Thus, the regulators have at least some limited influence on the structure of a group, when there are concerns regarding a proper ability of the authorities to supervise the group and the individual companies.

(g) Customer Protection measures.

Typically, in Germany there are no bank holding companies, and if so they will not have an operative business. If the holding company had an operative business, the consumer protection measures would not be different from the situation of a company which does not at the same time have holding functions. there are no specific consumer protection measures that would apply at group level.

(h) Specific questions

Question: E-Commerce market relevant matter - whether banks or bank holding companies or financial holding companies may hold a subsidiary which manages/conduct an internet shopping mall business while the bank itself only provides payment settlement services?

Answer: Yes, but depending on the size, prohibitively high capital requirements may apply (see above under B.5) because the internet shopping mall is unlikely to be regarded as a financial sector company.

Question: What kind of activities should be permitted for banks' subsidiaries or bank's relevant companies?

Answer: Under German law, restrictions aim at isolating and reducing risks which is a lesson learnt from the financial crisis. With that in mind, a qualitative rather than a specific approach should be applied. However, German law has no specific restrictions on the types of businesses that can be operated by banks' group companies. See above at 2.2 (e) for potential negative impact of certain activities on meeting the regulatory capital requirements on a consolidated basis. Nor have there been any particular lessons learned from the financial crisis in terms of specific risks resulting from nonfinancial activities of bank group companies.

Question: Outsourcing administrative business in connection with payment settlement services, which revenue would come from mainly third parties other than its parent banks? Under Japanese Banking Act, banks' subsidiaries or banks' relevant companies are imposed a requirement that requires such subsidiaries or relevant companies to earn its revenue of 50% or more from its parent banks.

Answer: There is no such provision under German law. In fact, bank's subsidiaries which offer payment settlement service (such as bcb - see fact sheet Deutsche Bank) offer their services to the banking sector as such.

Question: Please consider issue of anti-trust laws

Answer: It should be noted that sec. 7 ZAG is some kind of antitrust provision which deals with access to payment systems. The operator of a payment system must refrain from the following discriminatory activities:

- restrict access to the payment system with restrictive conditions or other unreasonable means
- treat participants unequally without a valid reason
- limit the participant's rights due to its institutional status.

Sec. 7(2) ZAG clarifies that the operator of a payment system is permitted to set objective criteria for participation in the payment system to the extent necessary to ensure effective protection of financial and operational stability and to avoid operational, performance risk and entrepreneurial risks.

However, sec. 7(4) exempts certain payment systems from the application of the antidiscrimination rules:

- Certain payment and settlement systems mentioned in sec. 24b KWG, because these are subject to separate antidiscrimination rules (discussed below);
- systems operated exclusively within a group of companies if there are equity links between the group members;
- systmns in which on single payment services provider or a group acts as payment services provider for payor and payee and is solely responsible for the administration of the system and other payment services providers are granted the right to participate in the system who are not able to negotiate remuneration between themselves, but each may set their own prices vis-à-vis payor and payee clients. This convoluted rule protects single operator

systems, such as three-party credit card systems or systems operated by telecoms operators or purely internal systems.

Sec. 24b KWG deals with certain payment and settlement systems that are subject to a special notification requirement. Sec. 24b(3) KWG provides that access to such systems must be granted to other CRR instituions under transparent and objective criteria. The right to reject a participant for valid commercial reasons shall remain unaffected.

2.3 Restriction on Foreign Banks

The Association of Foreign Banks has slightly over 200 members, although some members are not banks, but fund managers, finance companies or investment firms. The members include both "true" foreign banks who operate branch offices and Germany and local banks that are subsidiaries of foreign banks or foreign shareholders. By "foreign" we mean any country outside Germany.

According to Bundesbank, there are currently approximately 20 branches of non-EEA Banks, and 94 branches of EEA banks as well as 82 subsidiaries of foreign banks. Also there are 65 representative offices of foreign banks.

The landscape of foreign banks is very heterogenous and includes large and small banks, banks with a limited business model (such as trade finance or serving nationals of the country of origin or investment banks) and banks with a universal business model that competes with local banks.

As an example, JP Morgan has

- the Frankfurt branch of JP Morgan NA (the US parent bank)
- the Frankfurt branch of JP Morgan International Bank Limited (the UK bank operating on the basis of a EU passport) which is a subsidiary of JP MorganNA
- a locally licensed bank, JP Morgan AG, which is also a subsidiary of JP Morgan NA

(a) Permitted scope of business (direct sales, an agency and intermediary?)

The rendering of banking and financial services to customers resident in Germany is subject to a license requirement under the KWG, if the services are rendered commercially or on a scale which requires a commercially organized business undertaking. Already marketing activities with the aim to render the licensable services (i.e. before a commencement of business operations) trigger the license requirement. The license requirements under the KWG also apply in the case of a mere cross-border conduct of business from outside Germany without local presence if the institution is addressing (potential) customers with residence in Germany in a targeted manner. To that end, it is sufficient, if customers are merely addressed by means of distance communication (such as telephone or e-mail). BaFin has established this view in its guidance note 4/2005 (**BaFin Guidance Note**) and the view has been accepted by the German Federal Administrative Court and by the European Court of Justice (*European Court of Justice* **- "ECJ"**).

A foreign institution without local presence is exempt from the license requirement, if (i) it is contacted by potential clients on their own initiative (without any prior solicitation) and/or (ii) if merely existing customer relations are continued. In the second alternative (continuation of existing customer relations), also promotional activities going beyond the currently rendered services are generally covered by the passive services exemption (cp. BaFin Guidance Note).

(b) How can market be entered: necessary permissions and authorizations

EEA institutions have three options

- Incorporate a German subsidiary and obtain a German license in the scope required.

- Establish a branch office in Germany based on the rules of the European passport
- serve German customers on a cross-border basis without local presence based on the rules of the European passport.

The European passport regime has been part of various banking directives, currently CRD IV (Directive No. 2013/36 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms of 26 June 2013). The passport is an essential element to create a single market for bank business. It is available only to CRR institutions, but not limited purpose banks (other passports are available for investment firms, payment services providers and fund managers).

Given that supervision of CRR institutions is largely harmonized, there is no reason to submit banks to an additional license requirement when they become active in another country of the EEA. Therefore, banks may use their existing license and stay essentially supervised exclusively by their home state regulator.

Compared to the process for obtaining the initial license, the procedures for being able to do business in another member state are fairly easy.

For cross border services (Art. 39 CRD IV), the bank needs to supply its home member state authority with an application in which it states the Member State in which it intends to operate and a business plan which describes the investment services or ancillary activities which it intends to perform. This so called programme of operations is a condensed version of the bank's business plan and is particularly focused on the activities in the relevant host country.

The home state authorities will transmit the documentation to the authorities of the host state within one month of receiving the information and in case of cross border services, the bank may then start to provide the services in the host member state authority.

In the case of establishment of branch offices, the procedures set out in Art. 35 et seq. CRD IV are more or less similar, except that the period of passing on the information to the competent authority of the host member state is three months. In addition, the business may not be commenced immediately upon transfer of the documents to the host member state authority but rather upon receipt of a communication from the competent authority of the host member state. However, if the host member state does not make such communication, the bank is authorized to commence business within two months from the date of transmission of the documents to the host member state.

Contrary to the case of cross border services, where no additional requirements may be imposed by the host member state, in the case of branch offices, the host member state is responsible for the supervision of the branches in relation to certain obligations enacted in the general interest. In Germany this includes supervision of liquidity, million credits, the power to prohibit misleading advertising, the obligation to inform about the applicable protection scheme and certain limited reporting obligations apply. In addition, major changes regarding the operations and the managers must be notified to the BaFin one month in advance. Moreover, certain organizational obligations regarding the prevention of money laundering and terrorist financing will apply. It is important to note, that in contrast to non-EEA branch offices, the host state regulator cannot ask for a "dotation capital" (see below).

In case of perceived violations of the rules, BaFin will notify the home member state regulator. Only if the home state regulator does not take measures or such measures are insufficient, the BaFin can interfere with own measures. The same applies in case of urgencies.

In contrast, a large room for the application of home member states' supervision remains. For example, the home member state authorities have even the the right to carry out on-site inspections with the branch in the other Member States.

For a non-EEA institution there are four options:

- Incorporate a German subsidiary and obtain a German license in the scope required.
- Establish a branch office in Germany. From a supervisory law point of view the branch will be treated as a separate legal entity which needs to have its own funds ("**dotation capital**") and the branch manager will have to comply with the requirements for senior managers of banks.
- Incorporate a subsidiary in another EU/EEA country and “passport” the license to Germany under the “European passport” regime. As already discussed above, there are two alternative structures for the European passport: The cross-border passport and the branch office passport. In case of the cross-border passport the activities in Germany must be conducted on a mere cross-border basis, without any permanent physical presence in Germany. Alternatively, branch office passport to Germany can be used, in which case the activities could also be conducted via physical presence through a German branch office. However, in this case a larger number of German regulatory provisions would apply compared to the current cross-border passport.
- Upon application, BaFin can grant a discretionary exemption from the license requirement. The exemption is available if BaFin deems that there is no need for supervision, taking into account the nature of the conducted business. In case of foreign institutions, this generally only applies if the institution is effectively supervised in its home country by the competent authority in accordance with internationally recognized standards and the competent home country authority cooperates satisfactorily with BaFin (evidenced by a Memorandum of Understanding between BaFin and the home regulator). To that effect, BaFin requires a certificate from the home authority containing certain confirmations (see below Research 3 for more details).

(c) Supervision and regulation

If a German subsidiary of a foreign bank which is a CRR institution obtains a German license, supervision lies with ECB pursuant to Art. 4 (1) a. of the SSM regulation, BaFin and Bundesbank. Depending on the size, the bank will be subject to the full SSM mechanism or only to limited supervision regarding licensing and ownership control procedures (see Art. 6 SSM Regulation).

If a German branch is established by a non-EEA credit institution, local supervision solely lies with BaFin and Bundesbank. However, substantial requirements have to be met, including capital requirements as if the branch were a separate legal entity.

If the European passport regime is utilized by an existing EEA CRR credit institution, supervision lies with ECB and the regulator in the home country of the institution which passports its license abroad with only a limited range of German rules applicable. Again the extent of ECB supervision will depend on the size of the entity (Art. 6 SSM Regulation).

(d) Restricted activities

If a German subsidiary obtains a German license, 2.1 restrictions fully apply

If a German branch is established by a non-EEA credit institution, 2.1 restrictions fully apply to the extent contained in the KWG. Sec. 53 KWG also mandates compliance with certain CRR rules.

If the European passport regime is utilized, restrictions mainly result from restrictions in the institution’s home country. However, passported institutions may not involve in business not covered by the passport or which cannot be passported, such as deposit business. Also, the general restrictions of 2.1 apply.

(e) Using licensed banks agency services

Using intermediaries in Germany, such as introducing brokers, investment advisers, asset managers, etc., even if such intermediaries possess a German license for the conduct of such services will still be fully attributed to the foreign institution which cannot benefit from the intermediary's license and needs to have its own license.

This is because under the BaFin's administrative practice, any type of solicitation by a non-German bank directed at German residents will trigger a license requirement. Even if the foreign bank uses German intermediaries to solicit business from German residents, the activities by such German intermediaries will be fully attributed to the foreign bank. Therefore in most situations, using a German bank as a business introducer is not avoiding a license requirement for the foreign bank.

There is one exception, namely where the foreign bank operates in Germany on the basis of an exemption granted by the BaFin and wants to address German retail clients (see below Research 3 for a more detailed description of the exemption procedure).

With respect to retail clients, the foreign institution's activities' on the German market can only be exempt from a license requirement if it initiates the first contact through a German institution or a EEA institution which passported its license to Germany. Once contact is initiated, the foreign institution can continue to conduct transaction directly with the client.

Special rules apply to Swiss banks which are granted simplified access to the German market.

Furthermore, for CRR credit institutions from the EEA, the EU passport procedure is available, so that no local business introducer is required to conduct business with German residents.

For more details on agency bank structures, please refer to Research 3.

2.4 Current Status of existing banking groups, banking holding company groups and banks

(a) Fact Sheet Landesbank Hessen-Thüringen

(i) Business Description

Landesbank Hessen-Thüringen (Helaba) is the **largest German Landesbank (state bank out of nine state banks in Germany) by assets.** The Helaba Group **employs approximately 6,300 people and has a business volume of € 200 bn.** The key aspects of Helaba's business model are its **legal form as a public-law institution,** the **high proportion of ownership by the Sparkasse organisation** as well as the **retention and expansion of its activities in the S-Group and public development and infrastructure business.** Helaba's strategic business model centres on the three business units: **Wholesale Business; Sparkassen Group (S-Group) Business, Private Customers and SME** (50-100 employees; EUR 10-50 m turnover) **Business; and Public Development and Infrastructure Business.** Business is conducted both from the bank headquarters in Frankfurt am Main and Erfurt and from the branches in Düsseldorf, Kassel, Paris, London and New York. These are joined by representative and sales offices, subsidiaries and affiliates. With the exception of the subsidiary Frankfurter Sparkasse, the whole of the Helaba Group is organised into discrete divisions for operational and business control purposes, meaning that all product, customer and service units are managed on a standardized basis throughout the Group.

Helaba's activities in the **Wholesale Business unit concentrate on the six core business divisions of Real Estate, Corporate Finance, Financial Institutions and Public Finance, Global Markets, Asset Management and Transaction Banking.** In sales, Helaba follows two different approaches, firstly targeting product customers from the various product fields and, secondly, directing customer sales efforts across all products at major companies and the upper SME segment, institutional customers, municipal corporations and central, regional and local public authorities.

In the S-Group Business, Private Customers and SME Business unit, Helaba's strategic goal is to **strengthen its position as a leading S-Group bank for Germany.** In Hesse and Thuringia, Helaba and the S-Group Sparkassen make up the Sparkassen-Finanzgruppe Hessen-Thüringen, based on the business model of economic unity and a joint S-Group rating. In summer 2012, **comprehensive co-operation and business agreements** were entered into with the Sparkassen and their associations in North Rhine-Westphalia. In addition, there are sales co-operation agreements with the Sparkassen in Brandenburg. The co-operation agreements with the Sparkassen in North Rhine-Westphalia and Brandenburg complement the S-Group Concept of the Sparkassen-Finanzgruppe Hessen- Thüringen, which continues in its current form. Helaba is **one of the market leaders in the home loans and savings business in both Hesse and Thuringia through the legally dependent Landesbausparkasse Hessen-Thüringen (LBS).** Frankfurter Sparkasse, a wholly owned and fully consolidated subsidiary of Helaba organised under German public law, is the leading retail bank in the Frankfurt am Main region with over 800,000 customers; it also has a presence in the nationwide direct banking market through 1822direkt. Frankfurter Bankgesellschaft (Schweiz) AG and its wholly owned subsidiary Frankfurter Bankgesellschaft (Deutschland) AG provide Helaba's products and services for Sparkassen in the private banking and wealth and asset management segment.

In the Public Development and Infrastructure Business unit, Helaba has been **entrusted with administering public-sector development programmes of the Federal State of Hesse via "WIBank" – as a legally dependent entity within Helaba. WIBank,** which is exempt from corporate income tax and trade tax, enjoys the direct statutory guarantee of the State of Hesse as permitted under EU law.

Helaba has stakes in numerous other development institutions in Hesse and Thuringia too, most notably in guarantee banks and SME investment companies. Helaba has granted Thüringer Aufbaubank a subordinated loan of € 40 m.

(ii) Key Figures

	2013	**2012**
Total assets (in EUR bn)	178.08	199.3
Net profit (in EUR mn)	354	318
Tier 1 capital ratio	12.8%	11.2%
Cost-income ratio	61.6%	61.2%

(iii) Ownership Structure

Owners and guarantors of Landesbank Hessen-Thüringen are the Sparkassen- und Giroverband Hessen-Thüringen (85%) (Savings Banks and Giro Association of Hesse-Thuringia), the Federal State of Hesse (10%) and the Free State of Thuringia (5%). The governing bodies of the bank are the Owners' Assembly, the Supervisory Board and the Board of Managing Directors.

Helaba's public ownership structure as at 31 December 2013

Composition of share capital	in € m	in %
Sparkassen- und Giroverband Hessen-Thüringen (SGVHT)	405	68.85
State of Hesse	48	8.10
Rheinischer Sparkassen- und Giroverband	28	4.75
Sparkassenverband Westfalen-Lippe	28	4.75
Fides Beta GmbH	28	4.75
Fides Alpha GmbH	28	4.75
State of Thuringia	24	4.05
Total	**589**	**100.00**

(iv) Subsidiaries

Major subsidiaries

- 1822direkt Gesellschaft der Frankfurter Sparkasse mbH

  Distribution Company for direct banking products, 100 % subsidiary of Frankfurter Sparkasse.

- Frankfurter Bankgesellschaft (Schweiz) AG

  Private Banking and Wealth Management - Frankfurter Bankgesellschaft is a private bank headquartered in Zurich, Switzerland, and present in Germany with a subsidiary company based in Frankfurt am Main.

- Frankfurter Bankgesellschaft (Deutschland) AG

  Private Banking and Wealth Management - Frankfurter Bankgesellschaft is a private bank headquartered in Zurich, Switzerland, and present in Germany with a subsidiary company based in Frankfurt am Main. Also included in the Group are Nötzli, Mai & Partner Family Office AG and the fund management company LB Swiss (Investment) AG, both of which are based in Zurich.

- Frankfurter Sparkasse

  Retail business in the region of Frankfurt/Main - Frankfurter Sparkasse has a balance sheet total of more than 18.5 billion euros, making it the fourth largest savings bank (Sparkasse) in Germany. With approximately 100 branches, customer service centres and self-service terminals and more than 200 cashpoints, Frankfurter Sparkasse operates the most comprehensive service network in and around Frankfurt. More than 40 percent of the people of Frankfurt have placed their trust in Frankfurter Sparkasse for all their financial needs.

  As a modern, universal bank, Frankfurter Sparkasse provides all types of financial services for both private and corporate customers. It operates the largest network of branches and service centres in the entire region. Frankfurter Sparkasse is part of the Helaba Landesbank Hessen-Thüringen Group, the central S-Group bank for Hesse, Thuringia, North Rhine-Westphalia and Brandenburg.

Subsidiaries with non-banking services

- Real Estate/ Real Estate Management

- GGM Gesellschaft für Gebäude- Management GmbH
- HIB Helaba Gesellschaft für Immobilienbewertung mbH
- GWH Wohnungsgesellschaft mbH Hessen

- Economic Services

OFB Projektentwicklung GmbH (project development and the project management of high-quality major properties, concentrating on office, local government and commercial properties)

(b) Fact Sheet HypoVereinsbank

(i) Business Description

HypoVereinsbank[11] is part of one of Europe's largest banking groups, UniCredit. With total assets of EUR290 bn. (2013), a total workforce of about 19,000 and about 850 branch offices, **it is Germany's 3rd largest financial institution**. It is responsible for all of UniCredit's business in Germany while at the same time being the competence centre for international investment banking.

UniCredit Group is an **Italian global banking and financial services company**. Its network spanning 50 markets in 20 countries, with more than 9,000 branches and over 148,000 employees. Its strategic position in Western and Eastern Europe gives the group **one of the region's highest market shares**. In 2005, UniCredit merged with the German group HVB, which is itself formed in 1998 by the combination of two Bavarian banks: Bayerische Vereinsbank and Bayerische Hypotheken-und Wechsel-Bank. Integration with the HVB Group was reinforced by the merger with Bank Austria Creditanstalt in the year 2000 and enabled further growth for the UniCredit Group.

As a focused full-service bank, HypoVereinsbank carries out banking transactions of all kinds. The **Commercial Banking business segment** in Germany assists all clients in the **Private Clients Bank and the Unternehmer Bank business units** with any standardised or individual service or consulting requirement with many different kinds of banking services. The **Corporate & Investment Banking (CIB) business segment** aims to be the first port of call for **large corporate and institutional customers** who are looking for expert advice, quality products and processes and to create value.

HypoVereinsbank focuses on customer proximity through a **local sales organisation**. It has strengthened its regional responsibility further in 2013, allowing it to tap fresh growth potential on the German market.

HypoVereinsbank combines its deep and long-standing regional roots with a **Group-wide network of banks in 18 countries across central and eastern Europe and central Asia** in a way no other German bank does. All told, HypoVereinsbank is represented in around 50 countries worldwide via UniCredit. HypoVereinsbank sees itself as a corporate citizen going beyond the banking business and cultivates a social commitment in the regions in which it operates.

As a full-service bank, HypoVereinsbank offers all customer groups – **private and private banking customers, business, corporate and real estate customers and high net worth individuals and institutions** – a broad range of modern products and financial services.

The range of services for companies extends **from simple commercial banking products to the provision of capital market solutions**. Furthermore, access to the UniCredit group network in western, central and eastern Europe offers substantial added value especially to export-oriented small and medium-sized enterprises in Germany by supporting them in their international business activities.

[11] As of 15 December 2009, the Bank's registered name in the Commercial Register was changed from "Bayerische Hypo und Vereinsbank AG" to "UniCredit Bank AG". The "HypoVereinsbank" brand name is not affected by this change and remains in place.

In a modern multi-channel offering our **private customers have access to a personal relationship manager at their place of business**, to comprehensive specialist knowledge at all times and, if required, to an online branch with extended opening hours.

As an intermediary to the capital market, CIB helps corporate customers with their positioning, growth and internationalisation. **Three global product lines are elements of the integrated CIB value chain: Markets, Financing & Advisory (F&A) and Global Transaction Banking**.

(ii) Key Figures

	2013	**2012**
Total assets (in EUR bn)	290.0	347.3
Net profit (in EUR mn)	1,047	1,287
Tier 1 capital ratio	21.6%	17.8%
Cost-income ratio	63.6%	58.1

(iii) Ownership Structure

The stock capital of UniCredit Bank AG is held to 100% by Unicredit S.p.A.

(iv) Subsidiaries

<u>Major subsidiaries</u>

- DAB Bank AG

  DAB bank was founded in May 1994 and is listed on the Frankfurt Stock Exchange since 1999. DAB Bank AG is Germany's first discount broker. DAB Bank as direct bank provides a comprehensive product and service range around the themes banking, investment and trading. Its products provide solutions for savers, investors and traders. In corporate banking, DAB bank is a partner for asset managers, fund brokers, investment advisers and banks.

- Bankhaus Neelmeyer AG

  Bankhaus Neelmeyer AG provides various banking services in Bremen, Germany. The company offers retail banking, private banking, and corporate banking services to private, corporate, and institutional clients, as well as engaged in wealth management, international, and securities businesses. It serves trading enterprises, dependent persons and other private individuals, service enterprises, and non-profit-making organizations; and manufacturing, transport and communications, construction, financial services and insurance, and farming and forestry industries. The company is based in Bremen, Germany. Bankhaus Neelmeyer AG operates as a subsidiary of Unicredit Bank AG.

- UniCredit Luxembourg S.A.

  UniCredit Luxembourg S.A. provides private banking and investment advice services in Luxembourg. The company offers retail banking, corporate and investment banking, treasury, private banking, and financial and advisory services. It is also involved in the management of wealth for high net worth and ultra high net worth segments, as well as the asset management of life insurance policies. In addition, the company offers FiduNet, an online service for banks to trade fiduciary money in term deposits and call money; and CorpNet, an online service to corporate clients to trade term deposits and call money. It serves small and medium sized enterprises, large and multinational corporate clients, equity funds, and real estate clients. The company was formerly known as HVB Banque Luxembourg S.A. and changed its name to UniCredit Luxembourg S.A. in August 2009.

The company was founded in 1971 and is based in Luxembourg. UniCredit Luxembourg S.A. operates as a subsidiary of UniCredit Bank AG.

- direktanlage.at AG

  direktanlage.at is an Austrian online bank. In1995 started as an online brokerage pioneer in Austria, direktanlage.at since then offers the opportunity to invest in securities via Internet, phone and fax at all major exchanges in the world. Meanwhile, the product portfolio also includes traditional banking services such as checking account and savings account. The online banking points to a long history of success and currently services nearly 66,000 customers with a portfolio volume of EUR 4.1 billion.

- UniCredit Leasing GmbH

  With over 3,000 employees in 17 countries, UniCredit Leasing is among the leading companies both in the core markets of Europe and in the growth markets of Central and Eastern Europe. In 2009 the company recorded new business volume of EUR8bn. More than 100,000 customers were offered financial solutions for both mobile and immobile assets.

<u>Subsidiaries with non-banking services</u>

- Software
  - BaLea Soft GmbH & Co. KG
- Real Estate/ Real Estate Management
  - HVB Gesells.für Gebäude mbH & Co KG
  - Salvatorplatz-Gr.mbH & Co. OHG Saarland
  - Grundstücksgesellschaft Simon b.h.K.
  - TIVOLI Grundstücks-Aktiengesellschaft
  - Hypo-Bank Verwaltungszentrum GmbH
  - Salvatorplatz-Grundstücksgesellschaft mbH
  - Salvatorplatz-G.mbH & Co. OHG Verwaltungsgesellschaft
  - HVZ GmbH & Co. Objekt KG
  - Merkurhof Grundstücks. m.b.H.
  - Verwaltungsgesellschaft Katharinenhof mbH
- Economic Services
  - HVB Services South Africa (Proprietary) Ltd.
  - UniCredit Global Business Services GmbH (real estate services, procurement, HR Shared Service Center, Cash Monitoring and Middle Office)
  - HVB Secur GmbH (building security, events, personal security, consulting and conception)
- Hotel and Restaurant
  - Food & more GmbH

- Call Center for Retail Bank
    - ➢ UniCredit Direct Services GmbH

All Subsidiaries of HypoVereinsbank (UniCredit Bank AG)

https://www.unicreditgroup.eu/content/dam/unicreditgroup/documents/en/banking-group/organizational-structure/UniCredit_Banking_Group_Chart.pdf

(c) Fact Sheet DZ Bank

(i) Business Description

DZ BANK AG Deutsche Zentral-Genossenschaftsbank, Frankfurt am Main, is acting as **central bank, corporate bank and parent holding company of the DZ BANK Group**. Its objective is to **offer relevant products, exemplary services and efficient processes -** and thereby develop ourselves into a leading Allfinanz-Group.

As a **central bank** it serves as the subsidiary partner of approx. 900 local cooperative banks. It **conceives, develops and provides products and services aimed at every relevant customer segment** for the primary banks to market, and provides them with liquidity balancing and reliable refinancing management services.

As an internationally oriented corporate bank DZ BANK s**erves SME customers directly and provides them with the full range of Corporate Finance products to fund both operations and investments**. In Investment Banking, it is specialised in Fixed Income and private-customer-focused securities services. It puts the **exceptional placing power of the integrated cooperative financial services sector** to work at the interface between the capital markets and the custody account institutions. The International division provides a worldwide hub for the primary banks and their customers.

As a holding DZ BANK **coordinates the efforts of the cooperative sector's comprehensive range of specialised services in order to achieve synergies and grow market potentials** for the benefit of its local cooperative banks. Among others Bausparkasse Schwäbisch Hall, R+V Versicherung, Union Investment, DG HYP and VR Leasing belong to the DZ BANK Group.

In terms of the number of people, co-operatives are the **largest economic organisations in Germany** with approximately 20 million members. Co-operative banks represent the largest group of co-operative companies with 16 million members and 190,000 employees.

In the German cooperative financial network of approximately 1,000 co-operative banks in total, DZ BANK performs the **central bank function with WGZ-Bank** (WGZ BANK is the central bank of the people cooperative banks in Rhineland and Westphalia as well as a business and commercial bank). DZ BANK serves the local co-operative banks in Baden-Württemberg, Bavaria, Berlin, Brandenburg, Bremen, Hamburg, Hesse, Mecklenburg-Western Pomerania, Lower Saxony, Rhineland-Palatinate, Saarland, Saxony, Saxony-Anhalt, Schleswig-Holstein and Thuringia. This area covers more than three quarters of all co-operative banks in Germany. The co-operative banks are not only DZ BANK's most important customers but also its shareholders.

According to its statutes, DZ BANK's traditional mandate is to **promote the German co-operative system**. It supports its partner banks in times of high credit demand or of excess liquidity, and provides them with the whole multitude of products and banking services, because it would be inefficient to let every local credit co-operative develop these individually. Moreover, it is the central clearing bank, liquidity manager and service provider for the local co-operative banking sector. As a group it also covers business involving investments, mortgage banks, savings and loans as well as leasing, factoring, insurance and financing for equity capital and projects. These services are provided by specialists in the subsidiaries in Germany and abroad.

(ii) Key Figures

	2013	2012
Total assets (in EUR bn)	38.7	40.72
Net profit (in EUR mn)	1.47	0.97
Tier 1 capital ratio	16.4%	13.6%
Cost-income ratio	51.5%	60.7%

(iii) Ownership Structure

The shares of DZ Bank are hold by credit cooperatives (82.3%), WGZ Bank AG Westdeutsche Genossenschafts Zentralbank (6.7%,), other Cooperative Societies (6.9%) and others (4.1%)

(iv) Subsidiaries

<u>Major subsidiaries</u>

- DZ Private Bank

  DZ PRIVATBANK is the centre of excellence for private banking for the German cooperative banking group Raiffeisenbanken in Germany.

- Team!Bank / easy credit

  The Team Bank AG is a financial institution based in Nuremberg that sells installment loans and credit cards with built installment loan function under the brand easy credit. A major distribution channel are the cooperative banks in Germany.

- R+V

  The R + V Versicherung is one of the largest insurers in Germany for private and corporate clients and is part of Genossenschaftliche FinanzGruppe Volksbanken Raiffeisenbanken.

- Schwäbisch Hall

  Schwäbisch Hall is Germany’s largest Bausparkasse (Building Society) with the largest customer base in the nation. 7.3 million customers bank on and with Bausparkasse Schwäbisch Hall.

- Union Investment

  Union Investment is the expert in asset management in cooperative financial group.

- ACCENT Invest

  ACCENT Invest is a brand of DZ BANK for intelligent and flexible investment in co-operative banks in certificates.

- Reise Bank

  ReiseBank is with its 85 years of experience Germany's market leader in business travel payment.

- DG HYP

DG HYP is one of the leading mortgage banks in Germany and specializes in commercial real estate finance the cooperative financial network. Core competence is the commercial real estate financing. The focus is on the core segments of office , residential and retail.

- VR Equitypartner

  VR Equitypartner is one of the leading private equity financiers in Germany, Austria and Switzerland. It supports medium-sized family companies on a target-driven basis, underpinned by our decades of experience in solving complex strategic financing issues.

- dvb Bank

  The leading specialist in international transport finance.

- VR Leasing Gruppe

  VR Leasing Gruppe is the leasing subsidiary DZ Bank offers financing options. The product portfolio ranges from leasing, hire purchase and credit factoring up to central regulation.

- VR Corporate Finance

  VR Corporate Finance is an M&A specialist for the predominantly owner-managed Mittelstand. They advise clients on all equity-related matters, including the sale, acquisition or merger of a business, company succession planning, as well as structuring the financing of an acquisition.

<u>Subsidiaries with non-banking services</u>

- CardProcess

  CardProcess is a leading provider of electronic and cashless payment systems in Germany and has a unique range of services and technical expertise.

- dwpbank

  Deutsche WertpapierService Bank AG (dwpbank) is the leading securities settlement service provider for Germany’s financial market.

- Equens

  Equens is the largest pan-European payment processor, leading the market for future-proof payments and card processing solutions.

(d) Fact Sheet Deutsche Bank

(i) Business Description

Deutsche Bank AG is **one of the top financial groups in the world and the largest private bank in Germany**, where it operates about 2,000 retail branch locations. It has another 1,000 branches in more than 70 countries in Europe, the Americas, Asia, the Pacific Rim, and Africa. As of December 31, 2013, it operated 2,907 branches in 71 countries. Deutsche Bank AG was founded in 1870 and is headquartered in Frankfurt am Main, Germany. Deutsche Bank AG provides **investment, financial, and related products and services worldwide**, organized in 5 corporate divisions:

- Private & Business Clients

  PBC provides banking and other financial services to private customers, self-employed clients as well as small and medium-sized businesses in Germany and internationally.

PBC's product range includes payment and current account services, investment management and retirement planning, securities as well as deposits and loans. PBC is a leading retail bank in Deutsche Bank's home market, Germany, with a franchise in Italy, Spain, Belgium, Portugal, Poland and India. In China, PBC cooperates closely with Hua Xia Bank in which it holds a 19.99 % stake and is its second largest shareholder.

- Deutsche Asset & Wealth Management

DeAWM helps individuals and institutions worldwide to preserve and increase their wealth. DeAWM offers traditional and alternative investments across all major asset classes, as well as tailored wealth management solutions and private banking services to high net worth clients and family offices. DeAWM clients can draw on Deutsche Bank's entire range of wealth and asset management capabilities as well as a comprehensive selection of first-class products and solutions, also by third-party providers.

- Corporate Banking & Securities

CB&S consists of the Markets and the Corporate Finance Business Divisions. The Markets Business Division combines the sales, trading and structuring of a wide range of financial market products, including bonds, equities and equity-linked products, exchange-traded and over-the-counter derivatives, foreign exchange, money market instruments, securitized instruments and commodities. Corporate Finance is responsible for mergers and acquisitions, as well as debt and equity advisory and origination. Regional and industry-focused teams ensure the delivery of the entire range of financial products and services.

- Global Transaction Banking

GTB provides domestic and cross-border payments, risk mitigation and international trade finance for corporate clients and financial institutions across the globe. GTB also offers trust, agency, depositary, custody and related services.

- Non-Core Operations Unit

The Non-Core Operations Unit (NCOU) was established in late 2012 and is responsible for selling capital-intensive assets that are not core to the bank's new strategy, thereby reducing risk and capital demand. This also allows management to focus on strategic core operations and, at the same time, increases the transparency of external reporting.

- Central Infrastructure

The central infrastructure area comprises the Corporate Center departments Finance, Legal & Compliance, Group Audit, Tax, Risk, Investor Relations, Communications, Corporate Social Responsibility & Public Affairs, Human Resources, Group Technology and Operations, Group Strategy, Corporate Insurance and DB Research.

These support the Management Board through their **strategy, risk management and control functions**. Most of the processes required for this are **globally integrated into the business divisions**, but have their own independent reporting lines.

(ii) Key Figures

	2013	**2012**
Total assets (in EUR bn)	1.611	2.002
Net profit (in EUR mn)	1.456	814
Tier 1 capital ratio	16.9%	15.1%
Cost-income ratio	89.0%	92.5%

(iii) Ownership Structure

Excerpt from the Annual Report 2013 (data as of December 31, 2013):

Deutsche Bank shares remain almost entirely in free float. Around 99% of the bank's shareholders were private investors. BlackRock, Inc., New York, which holds 5.14% of Deutsche Bank's shares, is the only large shareholder whose holdings are subject to the statutory reporting threshold of 3%.

(iv) Subsidiaries

- Overview

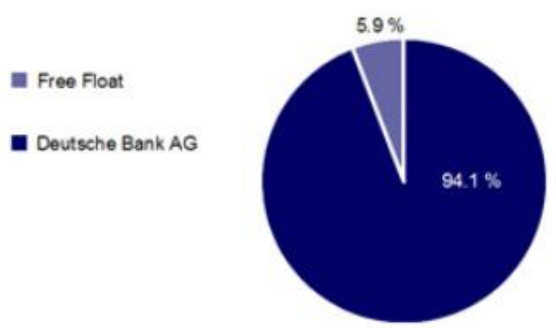
As of year-end 2013, Deutsche Bank's regulatory group comprised 844 subsidiaries, of which seven were consolidated on a pro-rata basis. The regulatory group comprised 127 credit institutions, one payment institution, 67 financial services institutions, 449 financial enterprises, 12 investment management companies and 188 ancillary services enterprises.

As of year-end 2012, Deutsche Bank's regulatory group comprised 913 subsidiaries, of which three were consolidated on a pro-rata basis. Our regulatory group comprised 137 credit institutions, three payment institutions, 80 financial services institutions, 514 financial enterprises, 14 investment management companies and 165 ancillary services enterprises.

- Postbank

  With around 14 million clients, 14,900 employees and total assets amounting to €155 billion, the Postbank Group is **one of Germany's largest financial service providers.** It focuses on business with private customers and with small and medium-sized companies.

  The Postbank Business Division comprises **consumer banking business** under the Postbank brand name as well as **DSL Bank, BHW Bausparkasse and norisbank**. With 14 million private and business clients and 5.2 million current accounts, Postbank continued to be a consumer banking leader in Germany. The overall positive business development is the result of Postbank reinforcing its business model and extending the successful **cooperation with Deutsche Post DHL**. The extended collaboration between the building societies BHW and Deutsche Bank Bauspar AG improved the bank's market presence in the home loans and savings business. While all distribution channels contributed to Postbank's performance, the business division significantly enhanced its online banking services in 2013. Nearly 35 % of Postbank's personal loan sales are now carried out online and almost 20 % of the new current accounts are opened online.



- Betriebs-Center für Banken AG

BCB, the Betriebs-Center für Banken AG, is a professional service provider for payment transaction services.

BCB operates multi-client platforms and employs staff with banking expertise. It offers full-service-solutions in our core-business area of **payment transactions.** The stake of PBC Banking Services GmbH der **Deutschen Bank in BCB amounts 100%.**

- Sal. Oppenheim

  Sal. Oppenheim is a German Private Bank, headquartered in Cologne. It manages and administers €138 billion of assets and has around 3,800 employees in more than 30 sites in Germany and Europe. Sal. Oppenheim is a private bank with more than 220 years of experience in wealth management, with focus on **asset management and provision of investment advice to private and institutional clients.** In 2010 Sal. Oppenheim became a **wholly-owned subsidiary of Deutsche Bank** and ceases its investment banking operations.

- Link to all subsidiaries of Deutsche Bank (Starting on Page 414)

https://annualreport.deutsche-bank.com/2013/ar/servicepages/downloads/files/dbfy2013_entire.pdf

Due to the sheer number of subsidiaries, it is not possible with reasonable effort to describe nonfinancial activities, if any, of Deutsche Bank's subsidiaries. All important subsidiaries set out above are engaged in financial sector activities and no nonfinancial activities are emphasized in the bank's annual report. Thus, we conclude that Deutsche Bank is not involved in nonfinancial activities of any meaningful size.

(e) Fact Sheet Commerzbank

(i) Business Description

Commerzbank is the **second largest German private bank** and a leading international commercial bank with branches and offices in more than 50 countries. The core markets of Commerzbank are Germany and Poland.

With the business areas **Private Customers, Mittelstandsbank, Corporates & Markets and Central & Eastern Europe**, its private customers and corporate clients, as well as institutional investors, profit from a comprehensive portfolio of banking and capital market services.

Commerzbank finances more than **30 per cent of Germany's foreign trade** and is the **unchallenged leader in financing for SMEs** (50-100 employees; EUR 10-50 m turnover)**.** With its subsidiaries comdirect and Poland's mBank it owns two of the world's most innovative online banks.

With some 1,200 branches Commerzbank has **one of the densest branch networks among German private banks**. In total, Commerzbank boasts approximately 15 million private customers, as well as one million business and corporate clients. The bank, which was founded in 1870, is represented at all the world's major stock exchanges. In 2013, it generated gross revenues of more than EUR 9 billion with approximately 54,000 employees on average.

The financial market and sovereign debt crisis has fundamentally changed the conditions for the banking sector. Commerzbank is **reacting in a consistent manner to this paradigm shift**: by reducing risks and optimising its capital base, maintaining its strict cost management and, at the same time, investing in the earnings power of the Core Bank by orienting its business model to the needs of its customers and the real economy.

Commerzbank invests in new products and services so as **to increase its earnings power**. In this respect they are orienting themselves towards the needs of their customers and towards their traditional values. They are **consistently gearing their business model** to this. In their Private Customers business they intend to **establish a modern multi-channel bank** which unites innovative technologies with traditional values such as fairness, trust and competence. In Mittelstandsbank they are continuing with a **successful business model** and **further expanding their market position at home and abroad**. In the Corporates & Markets segment they are positioning themselves to an even greater degree as a strong niche player. In Central & Eastern Europe, they are focusing on organic growth at mBank and developing its successful universal bank model.

Commerzbank has **given up the Public Finance, Commercial Real Estate and Deutsche Schiffsbank business areas**, and is in the process of cautiously reducing its portfolios bundled in the Non-Core Assets segment while at the same time taking care of its value. Thus they are releasing tied-up capital here - which will be used for growth in the Core Bank.

On the costs side Commerzbank has already seen an excellent development: as announced, they will realise the cost synergies in full from the Dresdner Bank (further information see 1.2)take-over. They are continuing their consistent cost management.

Commerzbank will thus **consolidate its position as a leading bank for private customers and corporate clients in Germany and Poland** on a sustainable basis even in a challenging environment.

- Take over of Dresdner Bank

2008 Commerzbank announces in August that it is taking over Dresdner Bank in two stages.

As a result of the **world-wide deep financial market crisis**, Commerzbank and the **Special Fund Financial Market Stabilization (SoFFin)** agree in December that the Special Fund will provide a silent participation in the amount of EUR 8.2 billion. In addition, SoFFin grants the Commerzbank Group a guarantee for debenture bonds for up to EUR 15 billion.

For the first time Commerzbank issues Exchange Traded Funds (ETFs) under the new brand "ComStage".

Hypothekenbank AG in Essen (Essen Hyp) and Eurohypo AG are combined.

Bundling of activities in Central and Eastern Europe in an individual Eastern European holding.

2009 The persistent financial market crisis increases the requirements for banks' capital resources. In January Commerzbank therefore decides to draw on additional equity in the amount of EUR 10 billion from SoFFin. After the transaction, the Federal Government holds 25% plus one share in Commerzbank.

The merger of Dresdner Bank AG with Commerzbank AG is entered in the commercial register on May 11.

Within the framework of the takeover of Dresdner Bank the cominvest Group is sold to Allianz.

Commerzbank is the first large bank to set up a customer advisory council.

Commerzbank opens its third Chinese branch in Tianjin.

Against the background of the expenditure for the integration and the still extremely difficult market conditions, Commerzbank closes the business year with a negative operating result of EUR 2.27 billion.

2010 At the beginning of the year Commerzbank combines its foundations with those of the former Dresdner Bank in a Foundation Centre.

The fourth Chinese branch is opened in Peking.

Commerzbank strengthens the rights of private customers and fixes important customer rights in a customer charter.

The equity fund initiated by KfW Bankengruppe and Commerzbank aims to achieve a sustainable equity reinforcement of small to medium-sized enterprises.

"Germany is turning yellow": in June the changeover to the new word and figurative mark begins. The new logo – the three-dimensional yellow ribbon – develops the figurative mark of Dresdner Bank further, combining elements of both traditional brands. This is backed up by the new brand promise "Achieving more together", which stands for the central values of partnership and performance.

Commerzbank passes the stress test of the European Banking Supervisors: in all scenarios the core capital ratio is far above the requirements.

One year earlier than expected, Commerzbank returns to profitability. The consolidated result amounts to EUR 1.4 billion.

2011 At the end of April Commerzbank concludes the IT integration of Dresdner Bank – after less than 1000 days. The IT systems of Commerzbank now process the data of 11 million customers.

Commerzbank repays EUR 14.3 billion of SoFFin's silent participation totalling EUR 16.2 billion.

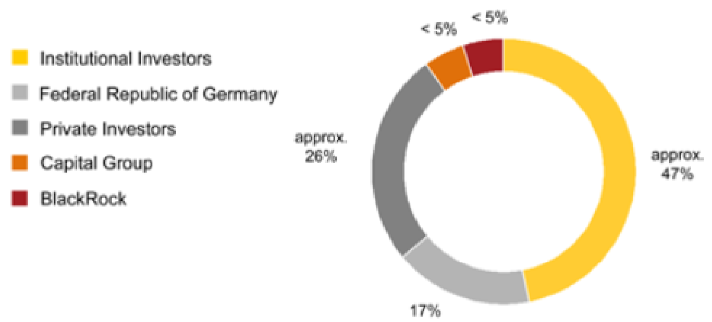
Announcement of the integration of Deutsche Schiffsbank.

The second stress test of the European Banking Supervisors, published in December, sees capital needs of EUR 5.3 billion. Commerzbank immediately adopts measures to ensure that the required corporate actions will be implemented by the end of June 2012.

(ii) Key Figures

	2013	**2012**
Total assets (in EUR bn)	549.7	636.0
Net profit (in EUR mn)	78	-47
Tier 1 capital ratio	13.5%	13.1%
Cost-income ratio	73.3%	71.3%

(iii) Ownership Structure



The major shareholder SoFFin (Financial Market Stabilization Fund) holds approx. 17%, Capital Group and BlackRock below 5%. In addition around a further 47% of shares are held by institutional investors.The proportion of private investors of whom the majority is based in Germany, amounts to 26% (as of december 2014).

(iv) Subsidiaries

In Germany, Commerzbank has some 1,200 branches.

Outside Germany, the bank is represented through

- 23 operational foreign branches
- 35 representative offices
- 7 material subsidiaries

According to ints annual report, Commerzbank considers the following to be its Germany major subsidiaries

- comdirect bank AG (an online bank)
- Commerz Real AG (the fund manager specialized on real estate funds
- Hypothekenbank Frankfurt AG (a mortgage bank)

Due to the sheer number of subsidiaries, it is not possible with reasonable effort to describe nonfinancial activities, if any, of Commerzbank's subsidiaries. All important subsidiaries set out above are engaged in financial sector activities and no nonfinancial activities are emphasized in the bank's annual report. Thus, we conclude that Commerzbank is not involved in nonfinancial activities of any meaningful size.

- Link to all subsidiaries of Commerzbank (Starting on Page 271)

https://www.commerzbank.de/media/aktionaere/service/archive/konzern/2014_2/Geschaeftsbericht2013_Konzern_EN.pdf

3. Others

3.1 Regulation of non-banks and subsidiaries of a banking/financial group providing Cash Management Services to corporations?

As a preliminary remark, there is no difference in the regulation of non-banks and (unregulated) subsidiaries of a banking/financial group in providing Cash Management Services. In particular, if a bank license is required for Cash Management Services, there is no specific exemption from the license requirement for (unregulated) subsidiaries of bank/financial groups.

(a) Regulation of Cash Management Services in general

(i) Cash Management generally

In larger groups of companies it becomes more difficult to manage cash properly. Some group companies may not have sufficient cash and have a borrowing need, while other group companies may have excess cash that they would normally deposit in a term deposit or otherwise generate interest income from the excess cash. However, since the interest income generated from the excess cash will be lower then the interest that will have to be paid by the other group company for the funding of a cash need, considerable savings can be achieved if the cash need of a group of companies is determined on an aggregated basis and excess cash is deployed with companies that have a liquidity shortage. In essence, the group would only deposit excess cash where such excess cash is available on an net aggregate basis and vice versa, a company would only borrow if there is a cash deficit on an aggregated basis.

The normal way to achieve that is by setting up a cash pool between all relevant group companies ("**cash pool members**"). In essence, one company would function as the central provider and borrower of cash within the group ("**cash pool leader**"). In other words the cash pool member having the excess cash would not directly lend the excess cash to a cash pool member which has a cash shortage but rather give its excess cash to the cash pool leader and the cash pool leader would lend the excess cash to the cash pool member which is in need of cash.

In order to achieve that, all positive cash balances and all negative cash balances on the bank accounts of the participating group companies will be set to zero at the end of each business day, i.e. all cash deficits on the accounts resulting from payout will be cured at the end of a day and all positive cash balances will be "sweeped"at the end of the day by way of cash transfer. The cash will be transferred to / from the account of the cash pool leader (very often the parent company of the group or a designated financing subsidiary).

If at the end of a day, the group has a cash shortage on a consolidated basis, the cash pool leader will make a drawing under an existing operating credit line or overdraft facility. If there is excess cash at the end of a day, the cash pool leader will reduce the existing borrowing under the operating credit line or overdraft facility and if the overdraft has a zero balance, he will invest the excess amount into short term deposits money market instruments or the like.

It is customary in Germany in such a scenario that the whole cash pool system would be set up with the help of a bank. Typically, all cash accounts will be held with the same bank so that it is easy to make a "sweep" of all accounts to zero balance at the end of a business day and to transfer the net balance to the target account held in the name of the cash pool leader and normally, the bank will manage the cash pool for the cash pool leader and also automatically provide extra cash under an overdraft facility / operating credit line or effect repayments.

Furthermore, in order to document the intercompany balances resulting from the daily cash sweep, a framework agreement will need to be set up on an intragroup basis that provide that any cash pool member whose positive cash balance is "sweeped" at the end of a day will have provided a loan to the cash pool leader. By the same token any cash pool member which has its negative account balance filled up as a result of the cash pool arrangement will be gained to have borrowed such amount from the cash pool leader.

Without going into too much detail, intragroup cash pools are not wholly unproblematic from a corporate law point of view. German company law for limited liability companies prohibits a repayment of capital to the extent that such capital is needed to cover the company's liabilities, i.e. any transfer of cash must not lead to a negative equity situation. This rule has been put in place because German corporations have a stated capital which serves as a safety cushion for the company's creditors. A German limited liability company (*Gesellschaft mit beschränkter Haftung*; "**GmbH"**) must have a minimum stated capital of EUR 25,000.00.

Similarly, a German stock corporation (*Aktiengesellschaft*; "**AG**") must have a minimum stated capital of EUR 50,000.00. In an AG, the protection of the company's capital is even stronger by providing that no payments at all must be made by the company to its shareholders other than dividends or liquidation proceeds.

German courts have interpreted the protection of capital provisions in a very restrictive manner so that also constructive repayments of capital are covered. As an example if the subsidiary repays the debts of the parent this will be viewed as indirect repayment of capital. The same is true where a subsidiary enters into an undervalue transaction with its parent company or with another company of the same group. In essence any financial benefit that flows back to the shareholder can be viewed as a prohibited repayment of capital.

Moreover, even the grant of a loan from the subsidiary to the parent could be viewed as a prohibited return of capital pursuant to the so-called "November decision" of the German Federal Supreme Court (BGHZ 157, 72, 75). In correcting the harsh consequences of the November decision, the statutory law was slightly relaxed and now allows for the grant of loans if the subsidiary has a "full-value" repayment claim against the parent. In essence, this means that the management of the subsidiary company must closely monitor the financial position of the parent company to determine whether its repayment claim has still "full value". If the creditworthiness of the parent deteriorates, the cash pool member should consider terminating the cash pool arrangement and the cash pool agreements must be set up in a manner that allow companies to terminate the arrangement in such scenarios.

The problem of a constructive repayment of capital does not arise where a domination and/or profit and loss pooling agreement is in place between the parent and the subsidiary because such an agreement overrides the capital protection rules in corporate law and provides protection in other manners (full assumption of all losses of the subsidiary).

(ii) Regulatory requirements for cash pooling and cash management

A clear distinction must be drawn between the services provided by the bank in the context of a cash management system and the services provided by the cash pool leader and by the participating members of the cash pool.

By providing the necessary accounts and by providing an over draft credit facility or operating credit line, the bank will be engaged in deposit business and lending business. Both activities require a banking license. No separate license for "cash management" services exists. Also, the bank is likely to provide payment services in connection with its cash management services.

As regards the cash pool leader and the cash pool members, the situation is similar, because when the cash pool leader makes a loan to the cash pool member it will be engaged in lending business. At the same time the cash pool member will be operating a deposit business. The same is true vice versa when the cash pool member deposits excess cash with the cash pool leader. In this case the cash pool leader will be operating a deposit business while the cash pool member may be engaged in lending business. However, all members of the cash pool including the cash pool leader will normally be exempt from the requirement of a banking license due to the fact that the German Banking Act contains a intragroup exemption. Details of the intragroup exemption and further exemptions are discussed in 3. below.

(b) Restrictions for banks in providing cash management services similar to the Japanese Banking Act

- Under the Japanese Banking Act banks are required not to provide more than 40% of the banks capital as financing
- Cash management service provided by bank could breach this requirement

How should the Banking Act be in light of this matter?

Under the EU Capital Requirements Regulation ("**CRR**") there are also large credit exposure limits. According to Article 395 CRR a bank must not hold risk positions the value of which exceeds 25 % of its own capital with respect to one single customer or a group of related customers, after taking into account credit risk mitigation. If the customer is another bank or belongs to a group of related customers which has at least one bank in the group, the risk position may not exceed 25 % of own funds or EUR 150 million whichever is higher. If EUR 150 million is higher than 25 % of the relevant own funds of the institution, the risk position must not exceed a reasonable upper limit that will be determined by the bank but, however, the limit of 100 % of own funds must not be exceeded.

That the large lending limits do not affect a number of risk positions, particularly regarding public sector debtors which have a risk weight of zero under the own funds requirements or risk positions which are secured by cash collateral or certain other liquid assets, but it appears to us that any such exceptions will not normally apply where a bank is engaged in cash management services for a corporate client. Furthermore, the competent authorities may exempt certain other assets from the requirements of the large lending limit (Article 400 (2) CRR) but, again, it seems that none of these would play any relevance in the definition of the lending limit connected to the operation of a cash management system with a large customer.

As a bottom line, we do not believe that German / European law provides any answers on whether it would be worthwhile to expand the ability of Japanese banks to offer cash management services to large groups of companies. To the contrary, it seems to us that European law is more restrictive than Japanese law by limiting the exposure to 25 % of own funds.

(c) Restrictions for intragroup loans similar to the Japanese Money Lending Business Act

German law provides for an exemption from the requirement to have a banking license for banking business performed on an intragroup basis. It is important to stress that under the relevant provision of the German Banking Act (Section 2 (4) No. 7) requires that such services are rendered "exclusively" with parent undertakings or their subsidiaries or sister companies. This means that one single transaction which is not covered by the intragroup exemption would destroy the exemption as a whole.

The terms "parent undertaking" and "subsidiary" are defined in the CRR, which in turn in its Article 4 (1) No. 15 and 16 refers to Directive 83/349/EC which defines a parent undertaking as an undertaking that has (i) a majority of voting rights or (ii) the right to appoint or remove a majority of the members of the relevant governing bodies or (iii) has the right to exercise a dominant influence over an undertaking of which it is a shareholder or member or (iv) which is otherwise controlled and vice versa, the entities so controlled are referred to as the subsidiary undertaking. Comparing such rules with the Japanese Money Lending Business Act, the German law is definitely more restrictive than Japanese law, because Japanese law also allows lending to joint venture entities in which an interest of 20 % or more is held. Also, there is no exemption for the case that the seller of a company may continue to provide loans to the sold company for some transition period after the closing of the sale of the subsidiary.

We note, however, that in our practice the restriction caused by the fact that no loans may be given to a former subsidiary after the sale of such subsidiary was sometimes making transactions more difficult, since funding by the (ex)parent company had to be replaced immediately upon closing of the transaction. Therefore, the potential change envisaged by the Japanese FSA would certainly also be welcome if implemented in Germany.

Nonetheless, a recent change of the regulatory guidance has thrown a fresh light on the need for a license.

Under the BaFin's guidance in force until spring 2014 instead of relying on the intragroup exemption it would be possible to provide the loan to a company in which a minority participation is held if the loan is made subject to a so-called "qualified subordination clause" (*qualifizierter Nachrang*). This means that the claim for repayment of the loan must be subordinated in a manner that when the company is making an insolvency test based on over-indebtedness, the debt to the shareholder will not count in making the calculation. In order to do so, the subordination must also be such that the shareholder debt ranks below all other creditors of the company who have not declared a subordination.

The German regulator changed its mind in the spring of this year by amending its guidance note regarding the definition of lending business and simultaneously also amending the guidance notice regarding the definition of deposit business. In relation to shareholder loans, the BaFin's guidance notice on deposit business says that the main point of qualifying a loan as lending business is whether there is an unconditional repayment claim. The BaFin now states that in the case of shareholder loans such a condition would result in principle from the corporate law duty of loyalty. Under such duty of loyalty a shareholder who has granted a loan to the company cannot enforce the loan repayment claim if as a result of the enforcement, the company would become insolvent. BaFin points to several statutory provisions in corporate and partnership law which indeed prevent such claim (Section 64 3rd Sentence of the German Limited Liability Act, Section 92 (2) 3rd Sentence of the German Stock

Corporation Act, Section 130a (1) 3rd Sentence of the German Commercial Code and Section 177a 1st Sentence Commercial Code).

As a result, the key consideration for qualifying a shareholder loan as regulated lending business is whether or not the shareholder will have an unconditional claim for repayment even when the company gets into financial difficulties or would get into financial difficulties if it had to repay the loan.

Thus, irrespective of whether the intragroup exemption applies, shareholder loans are no longer treated as lending business regardless of whether the shareholder is a "parent" undertaking. The only key requirement for loans to non-subsidiaries is whether the lender's claim is conditional or not, i.e. whether company law prevents a shareholder from making a repayment claim if this would render the company insolvent or if the company is already insolvent.

This new rule will also influence the case where the lender gives a loan to its former subsidiary in the context of a transaction, i.e. whether as a result of having ceased to be the shareholder of the subsidiary, he would now have an unconditional repayment claim. According to the prevailing view in the legal literature, also payments to former shareholders are subject to the condition that the company is not insolvent or would not be insolvent by the payment if at the time of making the loan, the loan creditor was a shareholder.

We also think that based on this view of BaFin, it would not matter if in the case example, the shareholder loan is not granted by the shareholder but rather by a subsidiary of the shareholder. Any loan repayment would be considered to economically benefit the shareholder and therefore also be subject to the repayment restrictions set out above.

3.2 Regulation of banking front services?

(a) General on the regulation of banking front services

- A provider has no banking license but in alliance with banks, provides customers payment facilities such as debit cards, or viewing payment histories, cash withdrawal from allied ATM etc.

  Generally speaking, it is possible subject to certain requirements, to operate a regulated business without having the necessary licenses by interposing a regulated institution that holds the necessary license for the business. In this case in the external relationship to the customer, a bank will appear as the contracting party although economically the customers will not be allocated to the bank but rather to the other cooperation partner who, within certain limits, has the ability to control the customer relationship. Such agreements can be found in a large number of cases on the German market. It is characteristic for such relationship that the bank does no longer take an entrepreneurial decisions in the individual case whether to establish, amend or terminate a client relationship. Rather this decision will be left to the cooperation partner in the framework of contractual agreements or in the framework of predetermined criteria. Hereinafter, a few examples are listed:

- Cooperation between the operator of a customer loyalty program and a credit card company in order to enable the customer to use the loyalty card with the logo of the operator of the loyalty program at the same time as a credit card. In this case the object of the cooperation is to obligate the credit card company to issue a credit card to the customer which frequently will have special features such for example specific insurance or the grant of bonus points in case of purchases made with the loyalty card / credit card. As a rule, when the cooperation terminates, the credit card company must pass on the customers to the newly nominated credit card company so that at the end, the operator of the loyalty programs controls the customers.

- Online P2P credit market place: The "fronting bank" will act as an interim lender in loan agreements which are concluded via an online market place provided that there are sufficient purchasers for the loan claim. In this case, the bank must undertake the obligation to sell the credit claim after the credit has been paid out to the purchaser. The relationship with the borrower, the bank shall remain entitled to collect the interest and payment of the principal amounts on behalf of the purchaser of the loan claim and to pass on collected moneys received to the purchase of the loan claim. The grant of the credit has been outsourced to the operator of the credit market place who will take the decision to grant the credit on behalf of the bank on the basis of predefined criteria (so-called "credit factory").

- Master Fund Manager: An asset manager who does not have the necessary license under the German investment fund law will pass his customer to a fully license fund manager who will set up a special fund negotiated between the asset manager and the customer. Moreover, the fund manager will appoint the asset manager as portfolio manager in the framework of an outsourcing agreement.

- White Label: Certain financial services for which a regulated or unregulated institution possesses no knowledge or no resources will be provided by another provider whose only role is to serve the customers of the first financial services provider. Even though the second financial services provider is the contract partner of the final customer, the service will not be distributed under the trademark or logo of the second financial services provider but rather under the brand and the logo of the first financial services provider so that superficially it appears as if the services was provided by the first financial services provider.

While one could argue that such an arrangements violate the corporate governance principles of the "fronting" institution, the arrangement is permissible under German banking supervision law if it is properly structured. It is true, that the fronting institution must keep full responsibility for the business entered into with its customers and it cannot delegate such responsibility to the cooperation partner who is the same "economic owner" of the business. Therefore, it is necessary that the services of the "economic owner" of the business is provided under an outsourcing arrangement that follows the rules on outsourcing set out in Section 25b KWG and AT9 MaRisk.

Outsourcing rules have been implemented in sec. 25b KWG and are concretized further in Part AT9 of the “Minimum Requirements for Risk Management” (*Mindestanforderungen für das Risikomanagement*; “MaRisk”) issued by the German regulator BaFin. Key requirements are as follows:

- Any outsourcing of a material function must be structured in a manner that avoids excessive risk, must not interfere with the proper performance of the business and services and must not impair a proper organization of the business.

- There must be an adequate and effective risk management in place which includes the outsourced services.

- The outsourcing must not lead to a delegation of the responsibility of the executive managers of the outsourcing institution

- The BaFin must not be impeded in the exercise of its supervisory tasks.

- The information and audit rights of BaFin must also extend to outsourced activities and processes also in case the outsourcing takes place abroad

- The statutory auditors and the internal auditors must have the same access and information rights

- The outsourcing agreement must be in writing and contain instruction and termination rights.
- AT 9 of MaRisk concretizes these obligations further as follows:
    - Need for a risk analysis by the outsourcing institution before outsourcing is agreed
    - Precautions are taken to safeguard continuity and quality of the performance of services and the outsourcing institution must examine its options in case of unintended or unexpected termination of the outsourced services (that includes, in particular, the need for a contingency plan in case the services provider goes bankrupt to be prepared by the outsourcing institution and a contingency plan prepared by the services provider to ensure the provision of services in case of disruptions such as fire, accident, loss of power etc.)
    - The services must be sufficiently specified.
    - The internal and external auditors must have information and audit .rights.
    - Instruction rights must be agreed "where necessary"
    - There must be contractual provisions safeguarding compliance with data protection rules.
    - There must be termination rights and adequate termination provisions (this normally includes provisions that secure continuity of services post termination).
    - The permissibility and modalities of a sub-outsourcing must be agreed, and in particular, the supervisory law requirements must be complied with also in case of sub-outsourcing.
    - The outsourcing provider must had information obligations in case of developments which could impair the proper performance of the services.

The outsourcing institution must continue to be able to adequately control and monitor the outsourced procedures, including a performance assessment based on defined criteria and a determination of clear responsibilities in the control and monitoring.

Based on compliance with such provisions, the fronting institutions will keep the ultimate control over the outsourced operations and makes sure that as result of the operations being performed by an external services provider the compliance with the regulatory provisions is not impaired and the competent regulator is able to continue to supervise the operations despite the fact that they have been outsourced to the economic owner of the business. Given that in such scenarios the economic owner of the business retains the economic benefit of the business (through suitable remuneration arrangements) these types of arrangements can be characterized as so-called "reverse outsourcing". In this case the economic arrangement is such that the "fronting institution" will only receive a remuneration for "lending" its license and for accepting the risks resulting from the outsourcing agreement and from being the fronting institution but the main economic benefits will be pass on to the outsourcing provider, e.g. by passing on all of the fees obtained from the clients to the outsourcing services provider with the fronting institutions retaining only a fee for its "fronting services".

However, it is important to understand that outsourced parts of the services are such that they themselves do not consist of a regulated but is only support activity.

The exemplary model where a provider has no banking license but provides customers with payment facilities such as credit cards, cash withdrawal or money transfers would probably be feasible in the same manner under German regulatory law. For a more detailed description of the business model we refer to the "SIMPLE" business model provided by the Japanese FSA.

In more detail:

(i) Issue of a debit card with the logo of the services provider

The card would have to be issued by a partner bank which at the same time operates a giro account for the customer which can be used to make payments. In this respect a direct contractual relationship between the customer and the bank must be established (issue of debit card and opening of a related giro account) Whenever the customer uses the card, the transaction amount would be debited from the bank account maintained with the issuing bank.

A cooperation agreement between the provider and the bank would establish the criteria under which the bank must accept the customers which the provider has solicited. Also, the cooperation agreement would stipulate that all customers nominated by the service provider will receive a card issued by the bank branded with the logo of the services provider. Moreover, the bank would undertake certain guarantees to make sure that the card which would issued can be operated at ATMs where cash withdrawals can be made for free.

(ii) Online payment transactions as well as online check deposit

It should be noted that checks have fallen out of use in the German market and therefore, such a service would certainly not be offered to German customers. Regardless, the cooperation agreement between the service provider and the bank would provide that the service provider provides an interface which allows the customer to access his bank account and to make money transfers from such account to another account.

It should be noted that this type of service (providing access to the banks electronic banking interface) is not currently a payment service. However, under the draft new European Payment Services Directive ("**PSDII**"), such intermediary services might be considered payment services in the future. There are a number of companies on the market which offer these types of interface services and handle potentially very sensitive customer data on payment transactions including passwords, PINs and TANs and such interface service form an integral part of the payment process. Therefore the EU Commission considers submitting these entities to payment services regulation.

(iii) Access real time information on all transactions using smartphones

See prior point. This would be providing an interface into the bank's systems to view transaction information the bank would outsource such access service to the service provider.

(iv) Other services

Other services such as useful apps or tools on the web to help budgeting and savings are not license business and can be provided by the provider directly to the customers under a contractual relationship directly between the provider and the customer.

(b) Authorization of bank fronting services for foreign banks' group companies in Japan

- Under Japanese Banking Act banks that wish to provide an agency or intermediation for the business activities of a foreign bank must obtain an authorization from the Prime Minister in advance for each foreign bank (before bank enters into contract to be entrusted with the foreign bank agency/intermediary service)

- Consideration to relax requirement: once an authorization is obtained for a foreign bank, then an authorization is no longer required for the foreign bank's group companies (reporting requirement is enough)

- How should the scope of the foreign bank's group companies be? (for example, is consolidated basis appropriate?

Under German banking supervisory law banks do not need any authorization to enter into outsourcing agreements with services providers on the basis of which they would act as a "fronting bank" for other parties. Therefore contrary to Japanese law, we see no restriction for a German bank to act as a representative for a foreign bank other than making sure appropriate arrangements are in place.

The non-EEA bank can, however, not solicit any direct contractual relationship with German customers unless it has obtained an exemption from the German banking license requirement. Under the BaFin's regulatory practice, even if initial contract to the customer is made by the fronting bank in Germany, the foreign bank would still be deemed to require a license as the solicitation efforts by the German agent would be attributed to the foreign bank and the foreign bank thus addresses itself to the German market in a targeted manner.

Pursuant to section 2 (4) of the German Banking Act (*Kreditwesengesetz* – "KWG"), foreign entities may be eligible for exemption from a licensing requirement. The legal requirement for an exemption is that "the entity does not require supervision, given the nature of the business it conducts" (for details see below 1.2). An exemption from a licensing requirement pursuant to section 2 (4) of the KWG can thus only be considered for cases in which the German regulator Bafin deems that no need for supervision exists in connection with the conducting of banking and financial services business generally subject to supervision .

In its guidance note 4/2005 on the cross-border rendering of banking and financial services (the **"BaFin Guidance Note"**) the BaFin has provided details on the application of the exemption to foreign financial institutions who wish to serve German residents on a cross-border basis.

As a rule, it is easier to obtain an exemption if the targeted customer base is limited to institutional clients. In this case, all banking transactions and financial services requiring a license under the KWG are eligible for the exemption.

BaFin deems the following to constitute institutional investors:

- the German federal government, federal states, local authorities and their institutions,
- credit and financial services institutions,
- investment (management companies),
- private and public insurance companies and
- companies which are not small enterprises, i.e. which exceed at least two of the following three criteria:
  - € 4.84 million in assets,
  - € 9.68 million revenues;
  - 50 employees.

All other clients are considered retail clients.

All banking transactions and financial services requiring a license under the KWG (with the exception of money transmission business) are eligible for the exemption with retail clients, provided the transactions are brokered through a credit institution within Germany. The same also generally applies if the transactions are brokered through an EEA institution, provided its license is comparable to that of a German credit institution and the activities of the EEA institution are covered by the so-called European Passport.

Following the initiation of the client relationship through a German credit institution or EEA institution, the company active in cross-border business can conduct (individual) future transactions directly with the client as part of the existing business relationship.

In general, there is no need for supervision if the institution is effectively supervised in its home country by the competent authority/authorities in accordance with internationally recognized standards and the competent home country authority/authorities cooperates/cooperate satisfactorily with BaFin.

The applicant company must submit a certificate from the competent authority/authorities of the home country confirming to BaFin that,

- the foreign entity concerned has been granted a license for the banking operations and/or financial services that it intends to provide on a cross-border basis in Germany,
- the commencement of the intended cross-border services in Germany raises no supervisory concerns and
- if such concerns should arise in the future, these will be reported to BaFin.
- To the extent that a non-EEA applicant intends to conduct cross-border business in Germany via branch offices in other non-EEA member states, the certificate shall also include confirmation that, there have been no problems in terms of cooperation with the competent authorities of the countries in which the branch offices are located, that no supervisory findings of fault have occurred with regard to the activities of the branches (to be listed individually) and that any subsequent problems or findings of fault will be communicated to BaFin. A detailed account must also be given of the extent to which sufficient supervision is maintained with respect, in particular, to company insolvency and money laundering prevention in the countries in which the branch offices are located.

BaFin may grant an exemption order if the institution does not require to be supervised because of the type of the performed business. Circumstances that the BaFin will take into consideration are, for example, type of business, customers and risks involved. In particular, where the activity triggering a license requirement in Germany is only ancillary to the main activity which does not trigger a license obligation in Germany, an exemption may be granted.

The application for an exemption must be submitted in writing by the company to BaFin. The application must be accompanied by the following documentation:

- copy of partnership agreement/articles of association;
- proof of company registration, to the extent that such registration is required;
- the most recent annual financial statements, including all related documentation (i.e. management report, auditor's report), to the extent that preparation of such documentation is required;
- certain personal information about the applicant or about each manager of the applicant company (board member/manager).
- a detailed description of the intended business activity, in particular to include an account of the specific transaction procedures and the intended market presence in Germany, depicting the client groups targeted; additionally - to the extent that it is relevant based on

the intended business activity - an explanation must be given as to how the money and securities transfer is to be accomplished;

- (sample) contract forms and (sample) agreements to be used for the intended business activities within Germany;
- appointment of a German receiving agent;
- certification from the competent authority/authorities of the home country.

In addition to the prerequisites described here, supplementary requirements may be added in individual cases by BaFin.

Alternatively if no exemption is obtained and the German fronting bank is the only contract partner of the German customer, the foreign institution could provide its services on a "back to back" basis by way of the "reverse" outsourcing arrangement describe above.

(c) Cashing out of Deposits

- In Japan only financial related companies may conduct the business of acceptance and withdrawal of bank's deposit through ATM
- Should it be permitted to conduct such service without using ATM? (for example at convenience stores)
- If a human is involved, how can the security be kept?

You have inquired whether it would be possible to provide a cash-out service outside of withdrawals via an APM, e.g. in a retail shop.

(i) Exemption for "reverse cash payments"

In our view the cashing out of amounts which will then be debited from an account maintained with the bank will be viewed as a payment services under Section 1 (2) No. 1 ZAG, namely "services by which cash deposits, other payment card or cash withdrawals from the payment accounts are enabled".

However based on the PSD, the ZAG contains an express exemption according to which a payee hands out cash to a payor in the framework of a payment transaction after the user of the payment services has explicitly asked for the performance of a payment transaction in connection with the purchase of goods or services (Section 1 (10) No. 4 ZAG). This service is referred to as "reverse cash payments" and releases retailers from the license requirement under the ZAG in line with article 4 lit. e PSD. This exemption shall catch cash-back services provided by merchants as point of sales, i.e. cash payments in which the customer pays without cash but pays a higher amount than he owes under the purchase transaction conducted in the shop of the merchant. The excess amount will then be paid in cash to the customer. In Germany these transactions are mostly done whenever a customer uses the his debit card in a retail shop. It should be noted that this exemption applies only if there is a close connection between a true merchandize transaction and the payout of cash. In other words, it would not be possible under German law to allow a merchant to disburse cash in the same manner as an ATM without the customer at the same time purchasing some goods with that merchant. Of course, it is conceivable that the customer purchases only a very small value item and obtains a relatively high cash amount.

(ii) Banking license requirements

While Section 1 (10) No. 4 ZAG provides a safe harbor for the retailers regarding the payment services license requirement under the ZAG, there is still an issue whether the retailer operates a lending business which would require a banking license under the KWG. In its guidance note regarding the definition of credit business, the BaFin has held that the cash-out at the store cash register by debiting a bank card or a credit card, even if only for amounts on top of a purchase of goods, could be considered lending business. However, BaFin also points out that this is not the case if the decision for making the payout of the cash is not taken by the retailer but is taken bindingly for the retailer by a license bank. A further prerequisite for avoiding the license requirement is also that no contract is created between the cardholder and the shop owner and that the payout is not qualified as a loan by the shop owner to the bank.

Applying this principle to the practical situation, it is quite clear that payouts made via debit card or credit card should be unproblematic and should not trigger a license requirement under the KWG for the retailer, because the card payments will be authorized by the issuer of the debit card or credit card via an electronic POS terminal.

One other way of using a debit card in Germany is the so-called direct debit method pursuant to which the card is only used to retrieve the account data for a direct debit transaction. In this case there is no guaranty that the bank account for which the direct debit is made will have sufficient cash and that the retailer will receive the cash-out amount from the bank of the cardholder. In such a situation, the decision to pay out the cash is taken by the retailer and not by the bank and therefore qualifies as credit business.

Finally, in its guidance note regarding the definition of credit business, the BaFin also states that it might be possible for the retailer to obtain an exemption from the license requirement under narrow circumstances. Essentially, the credit business would have to be a side business and not the main business of the retailer and be of such a nature that it does not require supervision by the BaFin. We have no information on the BaFin's practice regarding exemptions of retailers in this area. However, given that obtaining an exemption is a certain effort, we would highly doubt that this is a practical manner to allow small shop owners to enter into the business of cashing out on debit cards and that only large retail chains (such as supermarket chains) would undergo the effort of for obtaining an exemption. Also, we would expect that in order to avoid the lending risk, retailers would typically not use the direct debit method but rather use only the card authorization method. It should be emphasized that irrespective of the need for a banking license the German payment services law (in line with the Payment Services Directive) does not allow the payout on cards which is not connected to a purchase made with the card (see 3.1 above).

(iii) Agency model

However, there is also another possibility to allow a retailer to cooperate with a bank or payment services provider without requiring an own license. Section 1 (7) ZAG defines a so-called "agent" which is a person whose actions will be attributed to the payment services institution when executing payment services as an independent contractor in the name of a payment institution. In order to render payment services via an agent, the payment institution must submit the following information to the BaFin and the Bundesbank:

- name and address of the agent
- description of the internal control mechanisms which the agent applies in order to fulfill the requirements under the Money Laundering Act and
- the name of the senior managers and the persons responsible for the management of an agent which are used to render the payment services and evidence that these persons are reliable and have the necessary expertise (Section 19 ZAG).

Before using an agent, a payment institution must make sure that the agent is reliable and has the necessary expertise and that he will comply with the legal requirements when rendering payment services. Moreover, the institution must ensure that the payment services customer is informed prior or during the establishment of a business relationship regarding the status of the agent and, if applicable, the termination of that status. The institution must keep records on this due diligence exercise for a period of five years after the end of the status of the agent.

The BaFin can prohibit a payment services institution from using agents if it has not complied with its obligations under the ZAG to properly select or supervise its agents. This prohibition can relate either to individual agents or to using agents at all.

The BaFin can issue a regulation which specifies in greater detail type, scope and form of evidence required to assure reliability and expertise of the agent. On that basis the Agent Evidence Regulation (*Agentennachweisverordnung*; "**AgNwV**") has been enacted and provides a quite extensive list of documents that need to be submitted by the agent to the payment services provider before the agent can be recruited as follows:

- police record of the senior managers and the persons responsible for management
- current excerpt from the central register of businesses for the agent, the senior managers of the agent and the persons responsible for the management
- current excerpt from the register of debtors for the above named persons
- declaration of senior managers of the agent and the persons responsible for the management regarding the absence of certain convictions
- current certificates by the fiscal authorities for the agent, the senior managers of the agent and the persons responsible for the management regarding payment of taxes
- current information from the trade office regarding the agent
- current excerpt from the commercial register for the agent
- last annual financial statements or last statement of income of the agent as well as a current management accounts
- current evidence of registration as a resident for the managers of the agent and the persons responsible for the management
- Signed curriculum vitae of the managers of the agent and the persons responsible for the management without any time gaps which lists all education, professional and commercial activities
- the customary references and certificates evidencing trainings and education as well as professional commercial activities and
- evidence of any governmental permits which may be necessary based on the statement of activity made in the CV.

In case the information provided is incomplete, deficient or contradictory regarding one agent or a person acting for an agent the payment institution must proactively investigate and clarify the information. If needed further evidence must be obtained.

The AgNwV also states that the agents must have sufficient theoretical and practical knowledge of the payment services.

Section 2 AgNwValso requires payment institutions to make sure that agents continue to be reliable and have the necessary expertise and fulfill the statutory requirements and their information obligations by entering into a written agreement with the agent which specifies the obligations of the agent and the rights of the payment institutions including instructions and termination rights as well as audit rights in favor of the payment institutions and its auditors.

Given the relatively detailed requirements, it appears unlikely that small shop owners will undergo the procedures of becoming an agent, but it is at least a theoretical possibility for a cash payout service which does not require the retailers performing the payout to become licensed under the ZAG.