e-finance&payments law&policy

THE MONTHLY JOURNAL FOR THE ONLINE FINANCE AND PAYMENTS INDUSTRY
JUNE 2014 VOLUME 08 ISSUE 06
WWW.E-COMLAW.COM

US banking regulators to review laws

The US Federal Reserve, in collaboration with other banking regulators, announced on 4 June a complete review of laws affecting the financial sector with the goal of identifying particularly burdensome or outdated laws, and asked for comment in response to the first of several public notices.

"I think in reviewing which rules may be burdensome or outdated, the agencies should look at how the rules may be impeding the online/e-finance area," said Michelle Cohen, Member at Ifrah Law.

Three more requests for comment are to follow in the next two years, and rules that attract complaints for being too burdensome or outdated could be amended. "The public notice does not appear to have an emphasis on e-finance and online payments," explains Cohen. "However, it anticipates future notices, so e-finance and online payments could be addressed in the future."

"Experience has shown that agencies have responded positively to input from stakeholders about outdated and burdensome regulations," adds Cohen. "Changes can be made, but interested parties really do need to participate."

IN THIS ISSUE

UK's FCA initiative moves to support innovative start-ups

The UK's Financial Conduct Authority (FCA) announced on 29 May in a speech made by FCA Chief Executive Martin Wheatley at a Bloomberg conference, its Project Innovate initiative, which will offer compliance guidance to firms working on "positive developments" in financial innovation, and which will use FCA expertise to identify where the "system itself needs to adapt to new technology or broader change - rather than the other way round."

"I don't think that there is a particular 'trend' so much as an acceleration of development generally," said Dan Reavill, Partner at Travers Smith, discussing the drive behind Project Innovate. "We have seen this globally with the success of Kickstarter in crowdfunding, the emergence of Bitcoin as a viable virtual currency, and the growth of m-banking apps and peer-to-peer lending."

The FCA has created a hub within its policy team to assist firms, and has already begun discussions with start-ups. "This move has been generally well received," said Tim Wright, Partner at Pillsbury. "Smaller firms and start-ups can, in particular, be expected to benefit from the Innovate approach, which will encourage collaboration with the FCA in order to develop new technologies which are compliant from day one, with a regulatory environment which, instead of acting as a 'drag anchor,' supports innovation and encourages the 'brightest and most innovative companies to enter the sector.'"

The FCA will run an 'incubator' designed to support smaller firms in the run-up to regulatory authorisation, and will publish a scoping paper later this year covering *inter alia* effective support of innovation.

"It seems from Wheatley's message that the FCA does not want to constrain development within an existing regulatory framework which is either outdated, or ill-equipped to manage new technological challenges," said Reavill. "There will always be a legislative lag between the use of new technology and adaptation of the existing framework, but the keenness to adapt, rather than shoe-horn into existing regulation, is a welcome approach."

"Whether this marks a shift in the FCA's approach to digital currencies remains to be seen, with the regulator so far having kept a wide berth," said Wright. Reavill adds that "It will be interesting to see how the FCA manages the demands virtual currencies entail, especially as prominent companies begin to embrace 'non-traditional' payment methods."

US payday lenders file lawsuit against Operation Choke Point

The Community Financial Services Association of America (CFSA), the payday lenders trade association, and its member company Advance America, filed a lawsuit on 5 June accusing US regulators of adopting guidance that exceeds their statutory authority and using enforcement authority in an arbitrary and capricious manner, as part of Operation Choke Point.

"The CFSA seeks a court declaration that the FDIC, OCC and Board of Governors of the Federal Reserve System violated the Administrative Procedures Act and constitutional due process by issuing and enforcing guidance to banks as if they were rules against dealing with payday lenders," said Thomas E. Gilbertsen, Partner at Venable LLP. "The challenged pieces of guidance warned banks and provided suggestions for managing risks presented by certain third party relationships - including payment processors and their online merchants."

Operation Choke Point is a federal anti-fraud enforcement initiative targeting banks that provide online merchants and payday lenders with the means to process illegal transactions. "The DoJ anticipated that Operation Choke Point would also have the effect of causing banks to disassociate from customers engaged in lawful behaviour," said Peter Weinstock, Partner at Hunton & Williams. "The question is whether the government actions exceed their statutory authority or were arbitrary and capricious. Nonetheless, the CFSA has formulated a well-reasoned cause of action."

e-finance&paymentslaw&policy

THE MONTHLY JOURNAL FOR THE ONLINE FINANCE AND PAYMENTS INDUSTRY
VOLUME 08 ISSUE 06 JUNE 2014
WWW.E-COMLAW.COM

editorial board

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Associate Editor Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions Adelaide Pearce
adelaide.pearce@e-comlaw.com
telephone +44 (0)20 7012 1387
Design MadeInEarnest
www.madeinearnest.com

E-Finance & Payments Law & Policy is published monthly by Cecile Park Publishing Limited, 17 The Timber Yard, Drysdale Street, London N1 6ND
telephone +44 (0)20 7012 1380
facsimile +44 (0)20 7729 6093
www.e-comlaw.com

TPPs and the security of payment account access

In May, the European Forum on the Security of Retail Payments published its Final Recommendations on the Security of Payment Account Access. These Recommendations cover so called payment account access providers in which a third party provider accesses a customer's payment account to provide payment initiation or account information services, as these third party providers will become regulated under the proposed second Payment Services Directive. Steven Francis of Baker & McKenzie analyses the objectives and content of these Recommendations.

As is well known, the second Payment Services Directive is to include the creation of a newly regulated functionary, third party providers ('TPPs'). TPPs are essentially technology interfaces that offer, amongst other things, payment initiation services to consumers and merchants without ever taking possession of the funds to be transferred. They may also provide account owners with information on one or several accounts they have with one or a number of payment services firms. In providing payment initiation services, they offer, as the European Commission puts it, a software bridge between the website of the merchant and the online banking platform of the consumer in order to initiate payments on the basis of credit transfers or direct debits. TPPs are said to offer a low cost solution to those who wish to shop online but lack a credit card.

It has been noted that payment initiation services are some of the most important payment methods for e-commerce in some Member States. But the risk characteristics are different from non-TPP transactions because of the involvement of the additional party, the TPP, causing an increase in communications, directions and complexity. The additional party makes it harder to allocate responsibility in the event of fraud or error. The involvement of a TPP might make it more challenging to trace transactions.

The regulation of TPPs is controversial. One of the main purposes of the regulation of payment services firms is the safeguarding of client funds. But TPPs are no more than firms providing technical services without ever coming into possession of funds; some note that they are exempt under the current payment services regime and can see no reason to include them in its successor. Others take the view that, as TPPs come into possession of highly sensitive financial information about customers, it is crucial that there is effective supervision of them. The trigger for regulatory supervision must be properly judged: too light and customers may be put at risk, but too heavy and the costs for small businesses will become prohibitive.

With security firmly in mind, the European Forum on the Security of Retail Payments (the 'Forum'), in May 2014, published its Final Recommendations on the Security of Payment Account Access following a Public Consultation (the 'TPP Recommendations'). The TPP Recommendations complement the recommendations for the security of internet payments, which were produced by the Forum in 2012. The 2012 recommendations specifically excluded so called payment account access providers in which a third party provider accesses a customer's payment account to provide payment initiation or account information services: these activities are now provided for in the TPP Recommendations.

As the TPP Recommendations make clear, payment initiation services by TPPs differ according to whether or not the payee uses the service, and so is actively involved in preparing the payment initiation, and on how the authentication of the account owner is submitted to the account-servicing payment services provider.

The TPP Recommendations set out what is specifically excluded from its ambit, and many will be interested to see that digital or mobile wallets are excluded (but with the unhelpful proviso that the exclusion does not apply when the wallet is being used for payment account access services). The TPP Recommendations set out the objectives of the Forum as follows:

- TPPs should have security measures in place, similar to the level required by payment services providers and governance authorities (i.e. the entity responsible for the overall functioning of a payment scheme such as a card scheme);
- There should be sufficient transparency to enable customers (account owners and payees) to make an informed choice before and during the use of payment account access services;
- There should be traceability of all transactions and process flows so that it is clear which entity is responsible for the different parts of the process;
- There should be exchanges of information between those involved in a transaction;
- There should be no sharing of credentials between the TPPs and the account service payment services provider;
- The duration of payment account access should be

minimised, so reducing the risk of misuse of data; and

- TPPs and governance authorities, when providing services to e-merchants, should ensure (through technical restrictions or contractual provisions) that merchants comply with the necessary requirements.

It is said that the recommendations in the report are the minimum requirements. Each recommendation is accompanied by key considerations which provide much useful information and guidance, and TPPs, governance authorities and payment services providers should consider them carefully. Brief summaries of the recommendations are set out below, together with comments on omissions and matters of note:

Governance: TPPs and governance authorities should implement and review a formal security policy. It would be helpful if the TPP Recommendations added that the policy should be fit for purpose and that the parties should cooperate with each other and coordinate their respective efforts to ensure that it is operated satisfactorily by all.

Risk assessment: It is recommended that TPPs and governance authorities undertake security risk assessments. What is omitted though is that both should implement the findings of the assessment, and that the assessments themselves should be suitable and sufficient. Obviously, findings from the risk assessment should inform the matters covered in the policy.

Incident monitoring and reporting: This recommendation sensibly requires that the parties work together to investigate security incidents. There should though be an obligation to investigate major near misses (i.e. incidents that nearly caused a security, integrity or continuity of service issue but, fortuitously, did not).

The regulation of TPPs is controversial. One of the main purposes of the regulation of payment services firms is the safeguarding of client funds. But TPPs are no more than firms providing technical services without ever coming into possession of funds

Risk control and mitigation: Crucially there is a requirement that security measures be audited and that audit staff be independent of those on the business-side of the activity. While this is laudable it may well stretch the resources of a small TPP firm.

Traceability: TPPs, governance authorities and payment services providers should have processes in place so that all transactions and process flows can be traced. This will require coordinated effort, and so there should be an obligation imposed on the parties in their contractual documents.

Initial customer ID and information: Customers should confirm to the TPP their willingness to make use of payment account access services before being granted access. Merchants should properly be identified by the TPP.

Strong customer authentication: TPPs should ensure that the initiation of payments is protected by strong customer authentication. Strong authentication requires knowledge (password etc), ownership (e.g. token, smart card) and inherence (e.g. fingerprint).

Registration/enrolment: The delivery of authentication tools and/or payment account access-related software required to use the payment account access services must be undertaken in a secure manner.

Login attempts, session time out, validity of authentication: The TPP should have rules for payment access session 'time out,' to limit the number of log-in attempts and time limits for the validity of authentication.

Monitoring: Monitoring mechanisms to prevent, detect and block fraudulent transactions should be implemented. It remains to be seen how anti-money laundering controls will be applied to TPPs.

Protection of sensitive payment data: Sensitive payment data should be protected when stored, processed and/or transmitted.

Customer education and communication: TPPs should provide assistance and guidance to customers, when needed, with regard to customers' secure access to services and should communicate with customers in such a way as to assure them of the authenticity of messages received. TPPs should provide at least one secure channel for ongoing communication with customers concerning the correct and secure use of the payment account access services.

Notification, setting of limits: TPPs should set limits for their payment initiation services and could provide their registered customers with options for further risk limitation within these limits.

Customer access to information on the status of payment initiation: TPPs should provide immediately a confirmation to their customers of the successful initiation of the payment order with the payer's account-servicing PSP, together with information to check the correctness of the payment transaction.

While it is said that the same result may be achieved by means other than those set out in the TPP Recommendations, TPPs and governance authorities need to take account. Although not yet subject to the payment services' licensing regime, a failure to follow these recommendations may result in civil liability, depending always on the contractual framework in place.

Steven Francis Partner
Baker & McKenzie LLP, London
Steven.Francis@bakermckenzie.com

Implementation of the EMV standard marches on in US

Numerous retailers to roll out EMV acceptance in stores

On 15 January 2014, Al Franken, the Senate Chairman of the Committee on Privacy, Technology and the Law, sent a letter to Bank of America, Discover, American Express, MasterCard, Visa, Wells Fargo, JP Morgan Chase, Citigroup, and Capital One, stating that 'Adding security features, such as the chips in "EMV" cards that are used in most other industrialized countries may help prevent the breach of useable cardholder data and make it more difficult to commit payment fraud.'

Sen. Franken has requested that the foregoing institutions respond to him with the status of their transition to EMV cards, a description of the incentives to be utilised to encourage consumers and retailers to use more secure payment methods, and also that he be advised of the main impediments to the adoption of EMV cards and other security features.

On 30 May 2014, the California State Senate killed proposed legislation that would have required California retailers to implement the Europay MasterCard Visa ('EMV') smartcard standard that is generally regarded as less fraud-prone than the magnetic stripe technology currently in use. The legislation would have given retailers (other than gasoline station owners who had a one year delayed implementation date) until 1 April 2016 to put in place payment systems capable of supporting EMV debit and credit card transactions. Although the bill was killed, EMV implementation marches on from the standpoint of the payment card networks, issuers and merchants.

What is EMV?

EMV is a standard for the embedded microprocessor chip in each card that encrypts transaction data differently for each purchase. The standard, whether with chip and signature, or chip and PIN, should be more effective in preventing fraud and harder to duplicate than a magnetic stripe card. That said, having EMV acceptance at a point of sale may not prevent a data breach, but the data received may be of less value to a hacker. Rather than swipe an EMV card through a card reader, a cardholder will insert the card into a terminal that reads the chip and then asks for a personal identification number or prints out a receipt for a signature. The transaction information on a 'chip and pin' card is encoded uniquely every time, as opposed to the 'static' data contained on a magnetic stripe card, which is easier to duplicate.

As of April 2013, MasterCard, Visa, American Express, and Discover have required that acquirers, service providers, and sub-processors have the capability to process any EMV point of sale ('POS') transaction, both contact and contactless. To be fully compliant means that acquirers must adhere to payment network rules and complete approvals, including network approvals and testing procedures, in order to begin processing and passing additional authorisation messaging for EMV transactions. The major card networks have set an October 2015 deadline for United States card issuers, merchants, and merchant acquirers to be prepared for EMV. By that date, liability for counterfeit card fraud will shift to the party not equipped for EMV (other than gasoline dispensers which have a delayed implementation). But not everyone is waiting for the deadline.

In June 2014, Wal-Mart Stores Inc. announced that it will offer store-branded credit cards with EMV chips when it issues new cards this month (more than one year in advance of the payment card networks' implementation date). Other large merchants are moving ahead with the acceptance of EMV payments. Target reportedly is retrofitting its stores with EMV terminals and converting its REDcard credit and debit cards to the EMV standard for acceptance in early 2015.

However, having the terminals in place is only one piece of the puzzle; issuers must also move forward to replace mag-stripe cards with EMV enabled cards. In that Walmart and Target have publicly taken a position on the promotion of EMV enabled cards; presumably issuers (knowing their customers shop at such retailers) were determined not to wait for the deadline, but in fact, start issuing such cards in advance of the deadline. For example, Wells Fargo Bank recently announced that it will begin migrating all Wells One cardholders to EMV technology ahead of an October 2015 deadline, although it also announced it will maintain the magnetic stripe so that the cards will remain compatible with non-EMV terminals. JP Morgan Chase recently announced that it will replace certain Slate credit cards with cards that have an embedded chip and signature component (both for fraud reduction and as advertised, for greater acceptance outside of the US). The cards are to be replaced by 15 August 2014.

Of course, not all retailers will begin the migration. It could be a costly process to switch terminals and retailers with limited (or no) fraud may decide to bear the risk of liability (and PCI compliance) if they do not accept EMV capable cards. Furthermore, as reported, EMV capable cards prevent fraud at the point of sale, but reportedly are not successful in stopping fraud for card not present sales. Thus a smaller merchant, especially one that makes the majority of its sales through the internet, may determine that it simply does not make sense to comply with the payment card initiated deadline, and will take the wait and see approach. It would be ironic if smaller merchants, which prior to the deadline had not been the subject of fraud, are now the target.

It is anticipated that EMV adoption will significantly reduce fraud costs. Based on studies from those countries already utilising the EMV standard it certainly appears like a step (or more) in the right direction.

Barrie Van Brackle Partner and Co-Chair of the Global Payments and Consumer Financial Services practice group
Manatt, Phelps & Phillips LLP, Washington
bvanbrackle@manatt.com

Indonesia reacts to global trends with e-money regulation

Indonesia has taken notice of the global rise in electronic payment transactions and has developed its own electronic money regulation in response to the increasing importance of electronic payments. The Central Bank of the Republic of Indonesia has issued Bank Indonesia Regulation No. 16/8/PBI/2014, which contains key revisions to the earlier Amendment of Bank Indonesia Regulation No. 11/12/PBI/2009 concerning Electronic Money, as Bramantyo Pratama and Eldo Alwi, of Roosdiono & Partners, explain.

In the past decade, online payments have become increasingly important in the world economy to the extent that, according to the World Payments Report 2013 by Capgemini and RBS, mobile payment transactions are expected to grow 58.5% annually to 28.9 billion transactions in 2014. Electronic payment transactions are expected to grow by 18.1% yearly in the same period to a total of 34.8 billion transactions.

Meanwhile, according to Indonesia's national statistics authority (Statistics Indonesia), among the percentage of households that own/possess mobile telephones (in accordance with regional classification from the year 2005 - 2012), the utilisation of mobile phones in Indonesia increased significantly from 19.88% ownership in 2005 to 83.52% in 2012.

Observing the development of electronic money around the world, and given the very high number of mobile phone users in the country, the Central Bank of the Republic of Indonesia (the 'Bank of Indonesia') has issued Bank Indonesia Regulation No. 16/8/PBI/2014, with several key revisions to the earlier Amendment of Bank Indonesia Regulation No. 11/12/PBI/2009 concerning Electronic Money.

The revisions are in line with the Bank of Indonesia's stated aims, which are to decrease the utilisation of cash and help develop a cash-less society; to harmonise regulations concerning electronic money and the transfer of funds; to emphasise and clarify regulations on all aspects of electronic money, technology security, charges on electronic money transactions, transfer facility through electronic money, utilisation of part or entire electronic money value and the prohibition of exclusive partnerships for electronic money in public services; and to expand the payment and finance system through electronic money to support the National Financial Inclusion Strategy (Strategi Nasional Keuangan Inklusif.)

There are seven main revisions

First, Bank Indonesia now distinguishes between two types of electronic money: registered and unregistered. The registration of electronic money is intended to adopt the spirit of the 'know-your-customer' banking principle yet be aligned with anti-money laundering and terrorism laws. Hence, the Bank of Indonesia regulates the transfer of funds and cash withdrawal features for registered electronic money only, not unregistered electronic money.

Second, a non-bank institution is no longer required to obtain a money-remittance business licence. However, it is still required to obtain an issuer licence with a transfer or funds feature from the Bank of Indonesia.

Third, the Bank of Indonesia has applied a licensing period and limitation to the principal permit, issuer permit, acquirer permit, clearing operator and/or final settlement operator permit. While the previous regulation did not stipulate a licensing period, this new regulation prescribes a five year period (extension available) for any licence related to an electronic money principal, issuer, acquirer, clearing operator, or final settlement operator.

Fourth, electronic money may now be used for digital financial services.

Fifth, there is no limitation and exclusive partnership for the provision of electronic money for public services. Such public services include any services intended for the community such as transportation, electricity, health, and education.

Sixth, the Bank of Indonesia is now expressly providing protection to the user/holder of electronic money by the following measures: restricting electronic money issuers to determine a minimum value; charging costs for terminating the utilisation of electronic money; and/or unilaterally blocking the electronic money of a customer.

Seventh, Article 24A states that the Bank of Indonesia has the authority to request reports from electronic money operators that have not obtained a licence from the Bank of Indonesia.

Furthermore, any electronic money principal, issuer, acquirer, clearing operator, and/or final settlement operator is required to 'maintain, increase the electronic money security technology, and/or replace a more secure electronic money infrastructure and system.'

The DFS and the DFS agent

One of the major changes in the new regulation is the introduction of digital financial services ('DFS') within electronic money

transactions. An issuer may conduct DFS through cooperation with a third party ('DFS Agent') for the provision of payment service and financial system activities which utilise mobile based or web based infrastructure and technology for the purpose of financial inclusion. The DFS Agent can conduct the following activities: (i) as a facilitator in registering holders; (ii) providing top up for electronic money accounts; (iii) payment of bills using electronic money; (iv) cash withdrawal from electronic money accounts; (v) distribution of government aid programs to the community; and (vi) other approved facilities by the Bank of Indonesia. A transfer of funds operator or Indonesian legal entity and/or individual can act as a DFS Agent. Further, individual DFS Agents are only able to act as the DFS Agent of a Bank and conduct DFS for registered and online processed electronic money.

Financial inclusion and current obstacles

It is believed that the introduction of DFS will lead to the expansion of the electronic money market in Indonesia and increase payments that use the electronic money system because of the added convenience for potential users. The new facility for an issuer of electronic money to cooperate with DFS Agents is likely to provide unbanked and under-banked communities with access to secure financial services via electronic money. Indeed, in the future, the Bank of Indonesia intends for more people in remote areas to get connected and use electronic money.

The provision of electronic money by mobile phone providers should help people/consumers to conveniently browse and purchase (without the mobile phone providers needing to have other conventional bank-related products).

The registration of electronic money is intended to adopt the spirit of the 'know-your-customer' banking principle yet be aligned with anti-money laundering and terrorism laws

As also stated in the World Payments Report 2013 by Capgemini and RBS, mobile remittances and retail purchases through mobile phones are expected to form a major part of mobile payment transactions. In the report, the authors cite the examples of M-Pesa in Kenya and Fawry in Egypt, which provide bill payment services to enable easy money transfer and utility bill payments over mobile phones.

According to the permit registration data as listed by the Bank of Indonesia, eight non-bank institutions (including four telecommunication companies i.e. PT Telekomunikasi Indonesia Tbk, PT Telekomunikasi Selular, PT Indosat Tbk, and PT XL Axiata Tbk) have received licences as electronic money issuers.

However, public enthusiasm to use the current electronic money system has been low, especially in the transportation sector. The current Acting Governor of Jakarta, Basuki Tjahaja Purnama, has stated his disappointment with Indonesian society's apparent lack of interest in using electronic money to pay for city bus (transjakarta busway) and commuter train tickets. At the end of 2014, the regional government of DKI Jakarta plans to accept only electronic money payments for the transjakarta busway service. It is worth noting that the regional government is keen to support electronic money payments as a way to minimise possible corruption by transportation service providers, and improve public finance monitoring.

On another note, the Bank of Indonesia must expedite the issuance of the Circular Letter, the implementing regulation, so as to provide clear guidance on the implementation of the new regulation, for example to provide clear guidance on the aforementioned Article 24A.

Following the latest regulations, and given the very high rates of both mobile phone ownership and usage in Indonesia (while noting the slow but increasing trust in online and mobile security), it is likely sooner rather than later that electronic payments will grow significantly in the country. The new regulations will have a considerable impact on Indonesia's attractiveness as an investment destination and the knock-on effect of significant legislation such as this will ultimately likely cause an upward trajectory in terms of Indonesia's growth in the next few years. However, protection must be put in place to ensure that the regulations serve their purpose to the utmost extent.

Bramantyo Pratama Associate
Eldo Alwi Trainee Associate
Roosdiono & Partners, part of ZICO law
bramantyo.pratama@zicolaw.com
eldo.alwi@zicolaw.com

The FCA's competition review of the UK credit cards market

The FCA's review looks to protect consumers

Just two days after being officially appointed as the Chief Executive of the UK's Financial Conduct Authority ('FCA') on 1 April 2014 with responsibility for the consumer credit market, Martin Wheatley wasted no time in announcing that the FCA would be conducting a competition review into the credit card industry. On 6 June 2014, the FCA confirmed it will formally launch a study into the credit card market. This 'market study,' scheduled to take place at the end of 2014, has sparked little surprise in the eyes of the UK Cards Association, although market participants will undoubtedly be questioning what the FCA's agenda is despite Mr Wheatley's assertion that there are no "pre-determined terms of reference, outcome or agenda."

Protecting the vulnerable

The FCA announced in March 2014 that it planned to conduct a thematic review into payday lenders and clearly asserted that the credit card industry was being targeted to complement this review. Indeed, vulnerable consumers seem to be offered "what are akin to payday loans with plastic" and it is this group that will form the focus of the market study. Numerous statistics were reeled off to justify this, but to name a few: 30 million people in the UK hold at least one credit card and 3.7% of these make only the minimum payments on their credit cards for 12 months; StepChange (a charity) have said that around 10% of the people who visit it for advice, with an average of £27,000 of total debt, arrive with five or more credit cards; and gross spending on cards last year was £150 billion and there was around £57 billion in outstanding balances.

The figures do paint a gloomy picture of the vast number of so-called 'survival borrowers' who are using credit cards much the same as payday loans and to add further weight to the FCA's cause, it is worth reminding that the consumer credit helpline was overwhelmed with calls the day before the FCA became the regulator. However, the UK Credit Card Association responded with further facts in an attempt to brighten the picture:

- That credit card debt has actually fallen by £8.9 billion (13%) since 2008, whilst spending has increased by £26 billion (20%);
- Around 40% of credit card balances are non-interest bearing; and
- 59% of customers repay in full each month.

With respect to the FCA's focus on vulnerable survival borrowers, the FCA abides by its duty of care to consumers and the study will undoubtedly consider whether the market is taking advantage of this group and clarify whether competition is working in their interests.

Focus on competition

Whilst this study is framed as an exercise purely to protect consumers, it cannot be ignored that the FCA is set to receive competition law powers next April. It is difficult not to think that perhaps this is an information gathering exercise to prepare the FCA for its extended role. However, this focus on competition makes yet a further unsubtle comparison between the credit card market and the payday loans market. Indeed, the latter was referred to the Competition Commission for activities that the Office of Fair Trading ('OFT') suggested amounted to preventing, restricting or distorting competition. For some time, the industry has faced criticism in the face of potential anti-competitive activities such as the difficulty of comparing interest rates of different cards, excessive charges, and poor information about charges. Comments have gone further, attacking the industry for debt management practices and selling products that do not meet consumers' needs. Richard Lloyd, the Executive Director of Which?, cannot be ignored when he contends that "too may credit cards appear to be designed to catch customers out." A balance has to be struck between educating consumers to make sensible decisions and preventing credit card issuers from luring consumers to purchase products that are unsuitable for them.

Outcome of review

The FCA will use behavioural economics to review how consumers respond to the design, pricing and distribution of credit card products. Alongside this, it will look at whether customer inertia, irrationality or lack of willpower are significant factors in poor decision-making and indebtedness. The next steps will require a balance between the two. The FCA needs to consider this carefully to ensure that an unfair burden is not placed on market participants.

There is a need, undoubtedly, for credit card issuers to be more transparent about the terms on which they offer their products and to ensure that they make proportionate checks that products are suitable for consumers.

The founder of consumer website Fairer Finance, James Daley, also considers that the FCA may end long-term 0% balance transfer deals because such deals "are only commercially viable if enough customers trip up" as they are often subject to "excessive fees;" more general outcomes may include:

- Lines of credit limited to those already stretched through effective assessments of the ability to repay debt;
- Making the costs of credit entirely transparent at the point of sale; and
- New business models to ensure that risk is priced correctly to all borrowers.

The FCA will need to be careful that it does not regulate to make card issuers entirely responsible for ensuring consumers do not make poor decisions.

Dr. Nathalie Moreno Partner
Speechly Bircham LLP, London
Nathalie.Moreno@speechlys.com

Canada regulates prepaid payment products

On 1 May, the federal Prepaid Payment Products Regulations (the 'Regulations') enacted under the Bank Act, the Cooperative Credit Associations Act, the Insurance Companies Act and the Trust and Loan Companies Act, finally became effective in Canada. Prior to the enactment of the Regulations, there was a complete absence of any prepaid or gift card legislation in Canada that expressly applied to federally regulated institutions. Jacqueline D. Shinfield of Blake, Cassels & Graydon LLP shares her thoughts on the Regulations.

The Regulations provide a framework for prepaid payment products issued by federally regulated institutions. They impose specific disclosure requirements and contain restrictions on the expiry of funds and the imposition of maintenance fees. The Regulations are drafted to apply to a 'prepaid payment product' which is defined as a payment card, whether physical or electronic, that is, or can be, loaded with funds and used by the cardholder to make withdrawals or to purchase goods or services. Although the Regulations are thought of and described as consumer protection related, their scope is not limited to consumer cards.

Disclosures

Two sets of disclosures are required to be provided to cardholders under the Regulations; one set is to be provided in any documentation that the issuing institution 'prepares for the issuance of the product' and a second set is to be provided upon the actual issuance of the product.

Specifically, the Regulations require that before a prepaid payment product is issued, initial disclosures must be provided (i) in any document that the issuing institution prepares for the issuance of the product, including on the product's exterior packaging, if any; and (ii) in writing to any person applying to the institution for the product.

A few issues arise under this initial disclosure requirement. As a starting point, an institution needs to distinguish between its general advertising materials and those materials that it prepares 'for the issuance of a product' so that it can determine where the initial disclosures are to be made.

The Regulations also interestingly reference 'applying' for a product. While some prepaid products have application procedures, many do not. Clearly, where there is an application for a prepaid product, the initial disclosures are required to be included. Moreover, where there is 'exterior packaging' for a product the disclosures must be placed on that packaging as well. Because the Regulations, in referring to exterior packaging, use the words 'if any,' it is clear that an institution is not required to have any exterior packaging or exterior packaging disclosures. Rather, if an institution does have prepaid payment products that have exterior packaging, then, in such circumstances, the initial disclosures must be placed on the packaging.

The initial disclosures that are to be provided before a prepaid payment product is issued in the circumstances described above are as follows:

(i) the name of the issuing institution;

(ii) a toll free telephone number that can be used to inquire about the product's terms and conditions;

(iii) the following restrictions on the use of the product, if applicable:

- the fact that the product is not reloadable;
- the fact that the product cannot be used to make withdrawals; and
- any other restrictions that could reasonably be expected to affect a person's decision to acquire the product;

(iv) all fees that may be imposed in respect of the product;

(v) if the funds are not insured by the Canada Deposit Insurance Corporation, a statement to that effect; and

(vi) a statement in respect of the expiry of funds. For a prepaid product other than a promotional product, the statement must indicate that the holder's right to use the funds loaded onto the product will not expire. For a 'promotional product,' a statement is required that either the funds do not expire, or the day of which the right to use the funds will expire.

As noted from the disclosure requirement in (vi), in Canada a cardholder's right to use funds loaded on a prepaid product cannot expire unless the product is a 'promotional product.' The term 'promotional product' is defined as a product that is purchased by an entity and distributed as part of a promotional, loyalty or award program. If a particular program does not fit within this description then the program cannot be structured to allow funds to expire. In this regard, it is important to note that the Financial Consumer Agency of Canada (the 'FCAC'), the Canadian regulator, is interpreting this requirement in the context of commercial prepaid cards to mean that funds loaded onto promotional cards cannot expire vis-a-vis the entity that purchased the cards, however, they can in fact expire vis-a-vis the

cardholder.

Another important requirement in respect of the initial disclosures is that regarding the disclosure of fees, these must be presented in an information box and must prominently appear on any exterior packaging or other documentation. There are no specific font size or formatting requirements that are outlined for the information box. This lends itself well to mobile disclosures where size and formatting are not easily controlled.

As previously outlined, there are two sets of disclosures required. In addition to the initial disclosures noted above, additional disclosures are required to be provided to persons to whom a product is issued upon the issuance of the product. These disclosures are as follows:

(i) the product's terms and conditions, including rights and responsibilities for lost or stolen products;

(ii) a description of how a product holder can verify the balance of funds loaded onto a product;

(iii) a description of how a product holder can, in certain circumstances, use a product for partial payment of a purchase; and

(iv) the information noted above under the initial disclosure requirements, if this was not previously provided.

In addition to the initial and additional disclosures, the Regulations require that specific disclosures be placed on the product itself. For electronic products, these disclosures can be provided by electronic disclosure, at the product holder's request. The disclosures that are required to be placed on the product are as follows:

(i) the name of the issuing institution;

(ii) expiry date, if any;

The express consent requirement requires federally regulated institutions to implement processes and procedures to obtain the express consent of product holders for the charging of these fees

(iii) if it is a promotional product, the date on which the right to use funds expires;

(iv) a toll free number that can be used to make inquiries about the product (including balance inquiries and complaints); and

(v) a website address where all of the initial and additional disclosures can be obtained.

All of the disclosures discussed above are required to be provided in language, and presented in a manner, that is clear, simple and not misleading. This is in keeping with the clear language initiative of the FCAC as reflected in the FCAC's Clear Language and Presentation Principles and Guidelines for the Industry.

Prohibitions

Aside from the prohibition on funds expiry previously discussed, there are also restrictions imposed on increasing fees or imposing new fees on prepaid products. In this regard, the Regulations prohibit the introduction of a new fee or an increase in any fee associated with a prepaid payment product unless the holder of the product has provided the institution with his/her name and mailing or email address and the product holder has the ability to update such information. If an institution in fact has such information, then in order to add a new fee or increase a fee, the institution is required to:

(i) send notice to the most recent address of the product holder 30 days before the effective date of the increase or new fee; and

(ii) display the notice on the institution's website at least 60 days before the effective date of the fee increase or the imposition of the new fee.

Other prohibitions in the Regulations surround the imposition of maintenance fees. Specifically, an institution cannot impose a maintenance fee on a prepaid payment product for a period of twelve months from the date of activation unless the product is either a promotional product, or the product is reloadable and the holder has given their express consent to the imposition of the fee. As such, for non-reloadable cards, maintenance fees cannot be charged for a 12 month period from activation.

In respect of reloadable cards, express consent is required to charge a maintenance fee at any time before 12 months from activation. In respect of the requirement for express consent, previous regulatory guidance issued by the FCAC in other areas makes it clear that express consent requires some type of positive 'opt in' behaviour on the part of the cardholder; it cannot be implied from behaviour or through the imposition of terms and conditions that deem a product holder to be providing express consent. This express consent requirement requires federally regulated institutions to implement processes and procedures to obtain the express consent of product holders for the charging of these fees. In addition to the prohibition on maintenance fees, the Regulations also prohibit an institution from charging overdraft fees or interest on a prepaid product without the express consent of the product holder.

While the legislation came into force on 1 May 2014, unfortunately it did not provide any guidance or grandfathering on prepaid product inventory already in circulation prior to that date. This and other vagueness in the application of the legislation to commercial products is proving to be challenging for many issuers.

Jacqueline D. Shinfield Partner
Blake, Cassels & Graydon LLP, Toronto
jacqueline.shinfield@blakes.com

Montenegro looks forward to cross-border EU payments

Montenegro introduces new payment transactions law

On 8 January 2014, a new Law on Payment Transactions in Montenegro (the 'Law') entered into force. The Law is due to become applicable on 9 January 2015.

This new Montenegrin Law on Payment Transactions creates conditions for the advancement of a regulatory framework in the field of payment transactions. The improvement is reflected primarily in terms of the harmonisation with European Union legislation, with one of the main goals being to abolish differences between national and cross-border payment transactions with EU countries. Currently the law only defines payment transactions in the state, but when the new Law becomes applicable it will regulate cross-border transactions, their providers and the conditions for providing services. Cross-border transactions refer to the transactions between European Union states and Montenegro, when Montenegro becomes a Member State of the EU.

The list of authorised providers is expanded

In the earlier law on Payment Transactions, there were only two possible payment providers: the Central Bank and 11 commercial banks. Now, with new payment providers, banks have more competition, which will result in more effective and cheaper services.

The Law very precisely defines payment services and their providers. From 9 January 2015 the list of authorised providers will be expanded. Credit institutions (micro-financial institutions and credit unions), payment institutions and e-money institutions will be authorised to engage in payment services. This opportunity has also been given to the state and local self-government, but only on a commercial basis. Payment institutions and e-money institutions are completely new types of legal entities.

New legal entities – payment institutions and e-money institutions

The Law defines payment institutions as a legal entity which has a special licence for payment services issued by the Montenegrin Central Bank. A very important condition is share capital, which is necessary for approval. The minimum pecuniary share capital of a payment institution depends on the type of services the payment institution engages in. It can be €20,000; €50,000 or even €125,000. For the entire business, a payment institution must maintain funds above the amount of its share capital. Beyond payment transactions, some of the payment services institutions can also engage include: the execution of payment transactions, saving and processing, payment system operations and money remittance.

For users of payment services, the Law involves numerous mechanisms for funds protection. These include an obligation for a payment institution to provide safety for a client's money via an insurance policy or bank guarantee, keeping a client's money separate from the payment institution funds and numerous others.

According to the new Law, an electronic money institution is a legal entity holding a special licence issued by the Central Bank. This licence approves the e-money institution to issue electronic money. E-money institutions have to be seated in Montenegro. Their pecuniary share capital must be at least €350,000. Besides the issuance of e-money, electronic money institutions are allowed to provide other services related to e-money, but they can not take deposits. As in the case of payment institutions the Law provides numerous mechanisms for client fund protection for e-money institutions.

E-money

E-money is one of the novelties. The Law defines it as a deposited monetary value which is issued upon receipt of funds intended to be used for payment transactions and which represents a clients claim on the issuer and which is accepted by natural or legal persons different from the electric money issuer. E-money can also be issued by the Central Bank, commercial banks, credit institutions licensed in Montenegro, Montenegrin branches of foreign credit institutions, or state and local self-government if they are acting on a commercial basis.

Cross-border payment transactions

The new Law contains provisions regarding providing payment services in cross-border payment transactions. These provisions will be applicable once Montenegro becomes a member of the European Union. From that day, the Law allows EU-based providers to operate in Montenegro. Payment services in Montenegro, excluding Montenegrin providers, could be:

- Credit institutions based in some of the EU States, which have had a special licence issued by a competent institution in their home country;
- Payment institutions based in a Member State;
- E-money institutions based in a Member State; and
- European Central Bank and national Central banks based in Member States (if acting on a commercial basis).

Detailed licensing regulations, conditions of control for payment service providers, the number of pieces of information a service provider has to provide to the client and many other details in this law now provide transparency and security for users. During the period of adjustment, the Central Bank is going to enact implementing regulations, to get everything ready for 9 January 2015.

Milos Curovic Partner
ODI Law Firm Ilic, Serbia
milos.curovic@odi.rs

Protecting personal data in online financial services

In May the UK's Information Commissioner's Office ('ICO') published its guidance on 'Protecting personal data in online services,' which presents eight areas of computer security affecting personal data that have, as the ICO points out, 'frequently arisen during investigations of data breaches.' Stephen Bonner and Kirsten Mycroft of KPMG's Information Protection and Business Resilience team discuss the guidance - and the eight areas highlighted by the ICO - as it applies to financial services.

The guidance published in May by the ICO on protecting personal data in online services was certainly welcome, as there was a need for a clear, jargon-free guide that uses practical examples and sets out pragmatic steps - one that bridges, as far as possible, the gap between the IT specialists on the one hand and the privacy specialists on the other. That is essentially what we have here, and the ICO has, on the whole, done an impressive job.

The guide deals with eight areas of computer security affecting personal data that have 'frequently arisen during investigations of data breaches.'

The ICO acknowledges that there is a 'large amount of guidance already available in the wider field of information security' and that its report is not intended as a 'comprehensive manual' on the subject. Its intended audience is someone who is 'responsible for ensuring compliance with the Data Protection Act (DPA)' or for managing 'computing infrastructure' - whilst adding that those 'generally responsible for IT security' may also benefit from learning from the mistakes of others, which the report proceeds to set out examples of.

Its intended audience is actually a wide one, therefore. This is a good thing because traditionally privacy requirements have sat in the compliance or legal function, while the IT security team actually implement those requirements - often without fully understanding what the privacy team wanted. So something like this guide, which one could almost view as a traveller's or translation guide serving both sides - like a Berlitz guide to security if you will - can act as an important step in bridging the gap and making the dialogue more comprehensible to all parties.

Whilst there is a lot of guidance around already - to varying degrees of technical complexity - to an extent there was a vacuum that vendors of IT solutions would fill by selling point solutions that they assured their buyers would meet regulatory requirements. Now the regulator has set out clearly its expectations. It clarifies some of the 'reasonable' or 'appropriate' steps that need to be taken by organisations processing personal data online. Effectively, it has thrown down the gauntlet. There will be no wiggle room anymore because the ICO's expectations are spelled out here. That said, it has done a good job of not being too prescriptive - its recommendations are broad enough for organisations to interpret and implement in their own way. But - they must be implemented! And these really are minimum requirements, rather than being the high watermark. It will not be enough for a company to only meet these steps.

As personal data security is of particular relevance and importance in the financial services ('FS') sector, we will consider the eight areas that the ICO sets out from the perspective of that industry.

First on the list comes software updates. This is an entirely appropriate place to start. For example, GCHQ recently said that 80% of the most serious nation-level IT attacks use well-known flaws to gain access. Software updates - or software not being updated - is what causes the highest number of issues. It's basic, it's boring perhaps, but - a bit like eating your five a day or changing the oil in your car - it just needs to be done. Financial services firms actually do quite well here, to be fair. They are certainly much better than average. But it is not just about patching your core systems - you also have to think about apps like Java or Flash player on desktops, as well as mobile devices, Androids in particular, that can be plugged into the corporate network. Not only those, but with the advent of the Internet of Things, organisations also need to think about other assets like lighting, doors, access control systems, and photocopiers that have their own operating system or are controlled through servers which will also need updating. So there is work to do for everyone here to keep on top of the issue.

The second area on the ICO's hit list is SQL injection. This is something that by and large technical people understand and privacy people don't. Essentially it's when malicious instructions are inserted into databases. SQL injection is a fundamental cause of problems. It's actually easily avoided - but very prevalent. In a sense, it's the easily solved problem that we've never cracked, so it's good to see the ICO call it out here so high up the list. The guidance sets out different ways of dealing with it and gives its preferences which is helpful. By and large, FS organisations manage this issue

quite well centrally. It is harder though to keep visibility where systems and websites are run locally or through third party developers. Some FS clients are insisting that all third party developed software has proven secure coding.

The third area, unnecessary services, tackles one of the most basic and fundamental problems in IT security: everything comes turned on. When vendors supply solutions with everything turned on by default, it makes the attack surface area much bigger. The ICO has undeniably good advice here: turn off what you don't need. Malicious attacks often happen to services or solutions that companies weren't aware they had, or have never used. The most desirable thing to do here is to maintain a list of all your services. But this is something FS organisations in particular have no hope of doing: their environment is simply too large and too complex. They need to start by looking at the high risk areas first, those that are external-facing.

Decommissioning of software or services, which is the fourth area, deals with the next step - how to turn things you don't need off properly. Even things you don't need may contain large chunks of data that you need to keep or transfer to somewhere else - customer data that needs to be retained under data retention/privacy law for example. The guidance here is relatively technical and could perhaps do with a greater business services perspective if it is updated in the future.

Next comes one of the great bugbears of the industry - password storage. Whenever there is a high profile customer data breach incident - and they seem to be in the news regularly these days - this is something the industry worries about: how were the passwords stored? 'The passwords were encrypted' is always the defence line that is used. The guidance is quite prescriptive in its guidelines for storing passwords and migrating them from legacy systems - but will need to be updated as it very much reflects best practice now: things move on so quickly. Nor does it address one of the key questions: why are there so many password breaches? Why are they seemingly so easy to steal? This needs to be addressed. It is also noticeable that the guidelines put the onus on companies to educate their customers around choosing and using better, more difficult passwords.

Financial services firms are generally well-positioned against most of the eight areas, but certainly can't afford to let up and certainly still have work to do

Sixth on the list is configuration of SSL and TLS. For FS firms, this may be a surprise. We have never seen this to be the cause of a major issue. Certainly cryptography is an area that the financial services industry does well. For that reason, criminals almost invariably attack the customer's machine rather than the bank's end to crack communications. It's the customer end that is the more vulnerable. A question for banks though could be to what extent their internal services are similarly secure and encrypted.

The next issue is another big one - inappropriate locations for processing data. It's a very common cause of problems - from putting data on a laptop and losing the laptop to putting sensitive data on a website inadvertently. It's a difficult one to fix because it's all about the interplay between people, processes and technology. It's hard to detect and therefore hard to deal with. It's made harder by extended enterprises too - interactions with suppliers and third parties, integrating systems after M&A. It's good that the ICO has flagged it - but it's a difficult area to show that you are on top of.

The final area, default credentials, is an interesting one. If a solution comes with a default setting, should it be the responsibility of the buyer to change that setting as soon as they activate it - or should the responsibility be on the vendor to only enable it to be activated once the default setting has been changed? This is a good area for ongoing debate.

The guide therefore is a valuable distillation of hard-earned experience, and should be a very useful facilitator of discussions. Some of the controls may date quickly though, and Data Protection Officers ('DPOs') will need to ensure that they don't just slavishly apply these controls in future years without keeping up with the latest state of the art IT defences.

Financial services firms are generally well-positioned against most of the eight areas, but certainly can't afford to let up and certainly still have work to do - like everyone else - in some areas.

Finally, our suggestion for a ninth area of guidance? How to guard against shadow IT: areas of the business that have 'gone rogue' and implement something without IT security or privacy knowing. That's another frequent cause of problems and one that is hard for organisations to guard against.

Stephen Bonner Partner, Financial Services and Head of Information Protection and Business Resilience
Kirsten Mycroft Senior Manager, Information Protection and Business Resilience team
KPMG LLP, London
Stephen.Bonner@kpmg.co.uk

SEQR's view on the uptake of mobile payments

While many of the pieces of the puzzle are in place, mobile payments are yet to take off as completely as some industry commentators have speculated they should have by now. Alex Preece, UK Managing Director for the mobile wallet solution SEQR, part of global mobile payments company Seamless, outlines why he believes m-payments haven't reached their potential as yet and explains what in SEQR's view are the key components to achieving saturation, before analysing the environment for launching an m-payments solution in the UK.

We're seeing a fundamental change in how everyday people can pay for everyday things; this change will see mobile devices as a mechanism to enable much smarter and easier transactions. We see that the most important factors for this are already in place. The key is giving both retailers and consumers an incentive to be interested in wanting to abandon cards and switch to pay with their mobiles. Up until now, this incentive hasn't been possible.

The incentive for both consumers and retailers to abandon card payments on a large scale is about four major interacting components:

- Reducing costs;
- Faster and smoother processes;
- Added value; and
- Security.

With these as the starting points, it is easy to realise that we are facing a revolution in how we deliver payments. We have not seen anything like this since we went from paying by cheque to using a card to pay. This time however, because of the extremely large penetration of smartphones, it is almost an opportunity for an even faster transition. It is common knowledge that a large majority of phones sold are smartphones - the number is constantly increasing and in many markets, the proportion is as high as 90%. This development can be illustrated by the Capgemini World Payments Report 2013, which estimates that the number of mobile payments will increase by 62% in 2014 and by the end of the year will amount to 29 billion transactions for the year - and the trend is expected to continue. The analyst firm Gartner's analysis shows that the global value of payment transactions via mobile phones will reach $700 billion in 2017. This is a substantial market in which Seamless very much sees itself as a major contender.

Cost savings - key to breakthrough

If we begin by looking at the incentive to reduce costs, we note that in the past the incentives have not been strong enough for retailers to shift to mobile payments; this is because most of the offerings use the existing old infrastructure. Today's retailer is squeezed with low profit margins. Here, the card companies and the banks behind the card payments infrastructure have an unfair portion of the proceeds. Let us assume that a typical retailer is driven by a margin of 3-4% although in many cases it is even lower, especially if you're a supermarket. If the average transaction pays 1% (often much more) to the card companies and banks when customers pay with a card instead of cash, this equals 25-30% of profit. Card companies and banks have no reason to lower this, as it makes for a highly profitable business, and although we see that they are happy to participate in the transition to mobile payments, it is as long as they do not have to lower their fees.

By eliminating the intermediaries for retailers and simplifying the payment flow, the interchange being charged by card companies and banks can come right down. The level fees are set at is a fundamental piece of the puzzle as to why mobile payments haven't taken off yet. It is also an important reason why retailers - large and small - have shown great interest in our mobile payment solution, SEQR (se-cure). We offer merchants a 50% reduction in expenditure compared with the card companies, without the merchant needing to invest in any hardware, but rather, the merchant displays a QR code at the checkout, which also includes an NFC chip. This simplicity of scaling a mobile payment offering has contributed to how one of the three largest retail and wholesale companies in Sweden, Axfood (which owns supermarket chains Hemköp, Willys, PrisXtra and Tempo), could install SEQR at 2,400 points of sale ('POS') in less than two weeks. In 2014, SEQR was rolled out to all national pharmacy chain Apotek Hjärtat stores -1,300 POS in five days.

Disruptive technology

The reason we can half the expensive card fees is that we have our own developed proprietary transaction switch, which today manages billions of payments annually. This opportunity for hard-pressed retailers has helped gain a lot of interest, both in terms of those with physical and with online stores. Having a platform to address virtually all payment situations is also key; for example, enabling the sending of money to other bank accounts, paying and extending parking times or donating money to charities.

There are, however, lots of banks and markets that don't wish to adopt a simplified model but wish to keep the high fees in place and create something that is beneficial for themselves but not for retailers and consumers. This will hinder widespread adoption, and we hope that the Single Euro Payments Area ('SEPA') will help foster innovation and consumers can finally make the decision for themselves by opting for the best mobile payment solution. Here at Seamless we feel it's about giving the European market choice and creating a competitive ecosystem.

Added value

It is also important to remember that it is not enough that merchants want customers to switch to payments via mobile phones; consumers' own willingness to do this is also a prerequisite for success. It becomes extremely important that customers feel that it is easy, quick and secure to pay by mobile devices but also have a solution that adds value not offered through cards. Few people today leave home without their mobile phone and check it on average 150 times a day. Since we are already doing a wide range of tasks using our mobiles today, paying with it should be a natural step.

The convergence of all the vital pieces that make up a mobile payment is needless to say useless without consumer adoption. Enabling retailers to have their own loyalty programs is another key in moving people from paying with their cards to paying with their mobiles. From what we see, some mobile payment solutions don't make it any easier for the retailers and/or the consumers to make that transition. It's important to have everything in one place: account balances, all loyalty programs, coupons and deals but also tracking and logging receipts etc. Otherwise, it's not adding any value.

My belief is that we are in a period where the mobile phone is about to take over as the payment solution

Security

When we work with managing a consumer's money, security and reliability is of course paramount. Storing your credit/debit card in the phone is just another way of becoming a victim of fraud. It doesn't simplify the process nor does it make a mobile payment any more secure. To avoid this, SEQR has built a solution, independent from card infrastructure, in which the consumer does not have to hand over any information to the merchant, but all data will meet in our transaction switch. All transactions have to be approved by using one's personal PIN and all transactions are cleared online in real time. There is no way to make a transaction without the explicit permission of the user, therefore guaranteeing that a consumer will not be subject to risks similar to those card solutions bring.

My belief is that we are in a period where the mobile phone is about to take over as the payment solution. Cards are yesterday's solution and the current paradigm shift is comparable to when we went from cheques to cards. Because the penetration of smartphones is so large, this transition is going to be significantly faster.

The UK perspective

We're lucky that the UK is packed with very technically advanced retailers and savvy consumers, as well as a very high penetration of smartphones. Consumers, however, are at the mercy of the banks and the main infrastructure. Vocalink, which runs and maintains the whole payment system, is actually owned by the banks themselves, and even the Payments Council that is meant to be overseeing and helping businesses thrive within the payment ecosystem, is owned by the banks. This unfortunately limits the choice for retailers who don't get easy access to independent payment solution alternatives available on the market. There are countless retailers and a number of banks that want a solution that reduces fees, offers consumers a true mobile wallet, but more importantly works through all verticals and not just one. With the intermediaries cut out, banks still benefit from the transactions but without the merchants paying unnecessary fees. Our solution works for any bank, phone operator and merchant and we believe that it should be up to the consumer and the retailer to decide on what payment solution to use. As of today, more than 4,600 retailers in three countries have already chosen SEQR.

Alex Preece UK Managing Director
SEQR
alex.preece@seqr.com

The CFPB asks for feedback on GPR card disclosures

In the US, a number of consumer advocacy groups have raised issues with the fees and fee disclosures for prepaid cards, particularly general purpose reloadable ('GPR') cards. GPR cards provide services similar to a debit card, but without the bank account. These cards can be used anywhere the payment brand (Visa, MasterCard) is accepted, and can also be used at ATMs. Positioned as a substitute for bank accounts, many GPR cards also provide bill payment services and even 'convenience checks.'

In the US, the Credit Card Accountability Responsibility and Disclosure Act of 2009 (the 'CARD Act') limits the types and frequency of certain prepaid card fees, but exempts non-gift cards such as GPR cards. Therefore, issues about fee restrictions and disclosures are still ongoing.

The Federal Trade Commission Act (the 'FTC Act') generally requires that all consumer products have disclosures that are fair, clear and conspicuous. With respect to payments, Regulation E ('Reg E') requires clear and readily understandable disclosures regarding liability and unauthorised transactions, but Reg E has not yet been extended to all types of GPR cards. This summer, the Consumer Financial Protection Bureau ('CFPB') is expected to extend certain aspects of Reg E to additional types of GPR and perhaps other prepaid cards.

Beginning with the Advanced Notice of Proposed Rulemaking ('ANPR') issued on 24 May 2012, the CFPB made clear it was considering mandating the content and format of fee disclosures for GPR cards. In a 14 March blog post by Eric Goldberg, Senior Regulatory Counsel for the CFPB, the public got their first glimpses of two 'Model Form' CFPB-developed disclosures, as well as photographs of fee disclosures from current products. The post was issued in connection with a CFPB event where consumers were shown the disclosures and asked to provide feedback[1]. The Model Form disclosures contain:

- Certain fees are given more prominence than others.
- An asterisk is used on recurring fees in the chart and the bottom of the fee chart states 'Fee can be less depending on usage.'
- The statements - 'We charge other fees not listed here. See the enclosed account agreement or visit www.xyzprepaidcard.com/fees for details;' 'Until you register this card, your money is not protected;' and 'For more information about prepaid cards, visit consumerfinance.gov/prepaid cards.'

Comments posted on the CFPB blog seem to favour the first Model Form, but a number of comments state that the disclosures over simplify things. While one or more forms of the fee disclosures are expected to make it into the new regulations, the CFPB made it clear in the ANPR that it is aware that it will be difficult to have one disclosure that applies to all.

It is important to note that the CFPB is not requiring that all fees be included in the form disclosure. Instead, the consumer is referred to the account agreement and a website page for additional fee information. However, if a fee structure is at all complex, will the mandated content leave room for other information needed to clearly inform the consumer?

Additional issues that may be covered in the regulations include: Whether the fee disclosures are required pre- or post-sale or both; Whether the disclosures should include if the card balance is covered by FDIC insurance; and Whether an overdraft feature is included.

It seems that the CFPB feels the industry's pain in trying to make consumer-friendly disclosures on limited packaging. If its goal is to allow consumers to make 'apples to apples' comparisons of GPR card fees, however, the disclosures would seem to work for this purpose to the limited extent of the fees disclosed, provided the same Model Form is used for the products the consumer is comparing.

Once the CFPB has fully considered the comments and input received, it will issue a Notice of Proposed Rulemaking ('NPR') containing proposed regulations. Once published, there will be a public comment period before final regulations are issued. Assuming the NPR is issued this summer, final regulations are expected in 2015. However, if the CFPB makes significant changes to the proposed rules after comments are received, the final regulations may not issue until 2016.

Linda Odom Counsel
Bryan Cave LLP, Washington DC
linda.odom@bryancave.com

1. See http://www.consumerfinance.gov/blog/prepaid-cards-help-design-a-new-disclosure/