e-finance&payments law & policy

THE MONTHLY JOURNAL FOR THE FINANCIAL SERVICES INDUSTRY

OCTOBER 2012 - ISSUE 10

Philippines: cybercrime bill suspended

The Supreme Court of the Philippines issued a 120-day Temporary Suspension Order (TSO) of the Cybercrime Prevention Act 2012, on 9 October, following widespread protests that parts of the law are unconstitutional and threaten Filipino human rights.

The Cybercrime Prevention Act, designed to combat illegal online activity, took effect on 3 October, but since then has provoked a surge of criticism. Opponents disagree with the bill's strict provisions regarding alleged libellous content across social media, applicable to posts made before the law was passed. The Act makes defamation a criminal offense with jail terms of up to 12 years and website operators responsible for publishing defamatory material can be shut down.

"The Supreme Court is very likely to declare some provisions unconstitutional because they impinge on basic rights like freedom of expression," explains Dr. Erwin Alampay, Associate Professor at the University of the Philippines. "It is unclear whether this will lead to the repeal of just these provisions, or the entire law itself." The Supreme Court will now hear objections to the law.

IN THIS ISSUE

PCI SSC issues developers m-payment security guidelines

The PCI Security Standards Council (PCI SSC) released guidance on mobile payment acceptance security on 13 September, which sets out best practices for software developers and mobile device manufacturers on the development of adequate security controls to provide merchants with more secure mobile payment acceptance solutions.

"The purpose of these guidelines is to establish a common baseline of protection for cardholder data that transits through mobile devices," said Adam Atlas, Head Attorney at Adam Atlas at Law. But, continues Mark Taylor, Partner at Hogan Lovells LLP, "It's important to note that the guidelines are primarily that – guidelines to educate stakeholders, rather than outright standards."

The guidelines, developed by a PCI SSC industry task force, "start from the premise that mobile devices - be that smartphones, tablets or PDAs - are potentially higher risk than standard desktops and laptops," said Taylor, and as such set out guidance for securing payment transactions and the mobile application platform. "The particular focus of the guidelines is mobile devices which are not primarily a payment acceptance or point of sale device, but are being transformed into one through additional applications or hardware which operate on or interface with them," adds Taylor.

The guidelines set out three main risks associated with mobile payment transactions and three core objectives to address those risks. Key recommendations include: isolating sensitive functions and data in trusted environments; implementing secure coding best practices; eliminating unnecessary third-party access; creating the ability to remotely disable payment applications; creating server-side controls; and reporting unauthorised access.

A global industry standards body, the PCI SSC is made up of card companies, including American Express, MasterCard and Visa, which amongst other things manages the Payment Card Industry Data Security Standard (PCI DSS). The latest guidelines are part of a wider effort to increase mobile payment acceptance security.

"The guidelines are evolutionary rather than revolutionary, but will be helpful I think," said Taylor. "One of the concerns consumers have is security. The guidelines are unlikely to be the silver bullet, but should be useful in persuading consumers that the industry is serious about developing secure mobile payment solutions, which should in turn drive uptake by consumers."

Retailers oppose "realistic" interchange fee settlement

Six of the merchant plaintiffs in the interchange fee lawsuit between US retailers, Visa, MasterCard and US banks, are opposed to the settlement, voicing their concerns in a letter to Congress dated 20 September.

The plaintiffs described the $7.25 billion settlement proposed on 13 July as 'one-sided', claiming that the settlement continues to uphold the 'anti-competitive' nature of the US credit card market. The National Retail Federation (NRF) made its criticisms clear in a statement to the press: credit card companies are still not compelled to disclose card fees and may 'quickly recoup the cost of the settlement from retailers' through swipe fee increases 'that have averaged 16 percent a year over the past decade'.

Trish Wexler, a Partner at strategic communications firm VOX Global, however, called the settlement the "best and most realistic outcome possible for all involved." Michelle Cohen and Jeff Hamlin of Ifrah Law, agree that in their opinion, "The settlement terms do not appear to be patently unreasonable."

"The settlement's opposition continues to throw out tired arguments that were already considered in the course of the settlement negotiations," said Wexler, adding that "No court has ever ruled that the electronic payments system is anything but legal."

While the NRF is 'exploring the legal action [it] might take,' and US District Court Judge Gleeson will consider plaintiffs' views, Wexler is "highly confident" of the agreement gaining preliminary approval and believes Congress has "zero appetite" to step in.

e-finance&paymentslaw&policy

THE NEWSLETTER FOR THE FINANCIAL SERVICES INDUSTRY
VOLUME 06 - ISSUE 10 - OCTOBER 2012
WWW.E-COMLAW.COM

At a glance

UK – NatWest has suspended the use of its GetCash mobile app, which enables customers to withdraw cash without the need for a card, after dozens of customers report fraudulent practice.

USA – Online retailer Amazon rolls out loans service to small-business merchants.

Canada – The Canadian government claims it will be 'choosing carefully' the firms involved in the construction of a new secure communications network, triggering comments that the country is seeking to exclude Huawei, declared by a US panel to be a security threat.

EU – Information services firm Experian estimates that conversion to SEPA will cost European businesses billions of euros, as old payment errors are uncovered by the transition process.

UAE – Doha Bank has launched an online money transfer service allowing Dubai customers to send money internationally via multiple channels, including mobile devices.

Global – Capgemini's 2012 World Payment Report shows a 7.1 percent rise in e-payments in 2010, with the US identified as the biggest e-payments market.

USA – Bank of America is to roll out a payment app utilising QR codes in a North Carolina-based trial, in conjunction with mobile payment company Paydiant.

USA – Thirty banks will be targeted by Gozi Trojan viruses in mass cyber attacks this autumn, according to intelligence from security firm RSA.

UK – The UK Cards Association has reported a nine percent increase in total fraud losses in the UK card industry in the first half of 2012, with phishing attacks and deceptive practices at ATMs pinpointed as particularly to blame.

Japan & South Korea – Japanese wireless operator NTT DoCoMo and South Korean KT Corporation have finalised plans enabling customers to make NFC mobile payments in each other's countries.

UK – Barclays is to take over the online banking operations of ING in the UK.

USA – Retail giant Wal-Mart has teamed up with American Express to launch Bluebird, a mobile alternative to bank debit and current accounts.

editorial board

CECILE PARK PUBLISHING
Managing Editor Lindsey Greig
lindsey.greig@e-comlaw.com
Associate Editor Sophie Cameron
sophie.cameron@e-comlaw.com
Editorial Assistant Simon Fuller
simon.fuller@e-comlaw.com
Subscriptions Karl Nitzsche
karl.nitzsche@e-comlaw.com
telephone +44 (0)20 7012 1382
Design MadeInEarnest
www.madeinearnest.com
Print The Premier Print Group

Follow us on Twitter! **@EFPLP**

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
 ISSN 1752-6957.

Editorial

The FSA restructuring impact

Many will be aware that the UK government has introduced major reforms to the UK financial services regulatory structure. The main change is that the Financial Services Authority (the 'FSA') will be replaced by the Prudential Regulation Authority (the 'PRA') and the Financial Conduct Authority (the 'FCA'). The exact date for the change is as yet unknown, but likely to be in April 2013. In the meantime the FSA is already operating an internal 'twin peaks' model.

As a result of this regulatory reform, payment service providers will be directly affected. At present the FSA is the regulator for most aspects of the Payment Services Regulations 2009 (the 'PSRs'). In future the FCA will be the regulator responsible for the conduct of all firms currently regulated by the FSA, which includes payment service providers. The FCA will build on what progress the FSA has been able to make in recent months through more intensive supervision, earlier and more proactive intervention, and using enforcement to pursue deterrence. Payment service providers will therefore be placed under the supervision of a new type of regulator.

The precise supervisory approach is still under consideration, but details should be forthcoming as the FCA is due to publish its approach document at the end of October 2012. Martin Wheatley, Managing Director of the FSA and Chief-Designate of the FCA, has stressed to firms the importance of reading the FCA's approach document. At this point in time all that can be confidently stated is that that the supervision of firms will be more focused on conduct, particularly that of senior management. Key to the success of the new supervisory approach is ensuring that good consumer outcomes are placed at the heart of the business models of regulated firms.

At its core the FCA will focus on finding the most effective way to ensure the markets work well and delivering a fair deal for consumers. More specifically the FCA has been given strategic and operational objectives. The strategic objective is to ensure that 'relevant markets' function well. As payment services providers provide a regulated financial service, the market within which they operate falls within the scope of the strategic objective. The three operational objectives relate to consumer protection, integrity and competition.

As the operational objectives of the FCA show, consumer protection has been given significant importance under the new regulator. Payment service providers will have to secure an appropriate level of protection for its consumers. Whether this protection is in fact appropriate will depend on the FCA's assessment, having regard to a specified number of statutory factors that it must take account of. In a sense the FCA could be regarded as a champion for consumers in its attempts to make good customer outcomes a central consideration of the regulatory process.

The FCA's other objective to promote effective competition will also ensure good consumer outcomes. This competition objective does not however mean that the FCA is intended to be a price regulator, but its exact role in meeting the competition objective is still being considered. Broadly speaking what the competition objective will mean for payment service providers is that they will be expected to compete for business by offering better services, better value and better products suited to their clients needs. A consequence of this focus on competition could be that payment service providers have to create and develop different ways of providing services. The most successful firms in this market will therefore be those who are able to accurately and effectively address consumers' needs in the most appropriate manner.

In order to meet the competition objective the FCA will gain new powers to ask the OFT to consider whether features of a financial services market prevent, restrict or distort competition. So it may be deemed necessary to restrict certain practices used in the payment service market by providers to give them a competitive edge, but that upon closer inspection do not actually promote competition. Such practices may not be overtly anti-competitive hence why the FCA is expected to undertake thorough studies of the relevant markets.

It is abundantly clear that the biggest change payment service providers, amongst others, will have to adjust to is this move to a more pre-emptive approach. The introduction of the FCA will see a change from a reactive regulator, as the FSA traditionally only involved itself after problems arose, to a proactive regulator that will try to identify risks and deal with them before they can become big problems that affect consumers. To fulfil its brief the FCA will make forward-looking judgements based on firms' business models and strategies. As a result payment service providers can look forward to being more regularly assessed.

William Long
John M. Casanova
Sidley Austin LLP
wlong@sidley.com
jcasanova@sidley.com

A consultation: setting the strategy for UK payments

In July 2012 HM Treasury published its consultation 'Setting the strategy for UK payments' inviting views on 'options for reforming the regulation and governance of payments networks in the UK'. Kate Johnson, an Associate, specialising in payments in Osborne Clarke's Financial Institutions Group, discusses the context surrounding the consultation and the UK Government's approach to setting a strategy for mobile payments.

The Treasury's Consultation (the 'Consultation') was triggered in the most part by the decision taken by the Payments Council in 2009 that cheques should be phased out by banks and building societies from 2018 and the subsequent retraction of this decision following concerns around the impact of cheque withdrawal (in the absence of viable alternatives) on particular parts of society. The cheques decision prompted the Government to look closer at the Payments Council resulting in the Consultation whose aim it is to improve the way that payments strategy is made in the UK.

The Payments Council

In 2007, the Payments Council was founded as an organisation whose main objectives are broadly:

- Strategic vision: to lead the future development of co-operative payment services in the United Kingdom in order to ensure that payment networks as a whole meet the needs of payment service providers, users and the wider economy;
- Openness and accountability: to ensure that payment systems are open and accountable; and
- Integrity: to ensure the operational efficiency, effectiveness and integrity of payment services in the United Kingdom.

The Government has no concerns about the stability, reliability and efficiency of UK payments systems. Its key concerns, and why it believes change is required, is that it does not believe the Payments Council has, to date, been as successful as originally intended in developing new and existing services, ensuring payments networks operate for the benefit of all users and in effectively communicating its decisions.

The Consultation

The Consultation sets out three options for reconfiguring the existing payments regime in order to meet Government's aims and seeks responses on a number of questions relating to each option. Although three options are outlined, it is made quite clear within the wording of the Consultation that Options 1 and 3 are not, in HM Treasury's view, options at all and that its strong preference is for the implementation of Option 2.

So what are the options?

Option 1 - this proposes a range of reforms which could be carried out within the existing Payments Council governance framework to improve the way it delivers the Government's aims, essentially enhancing self-regulation. One of the main aims of the changes would be to make the Payments Council more responsive to the needs and views of end users, including consumers. It would include amending the composition of the Payments Council Board to strengthen the voice of consumers among the independent members and ensure any two of the four independent directors could veto a decision made by the Board. This option would not bring about any increased regulatory oversight (and associated regulatory burden) to payments strategy in the UK, but would be the cheapest of the three options to implement.

Option 2 - the second option includes the proposed creation of a new public body (known as the Payments Strategy Board, or 'PSB') to set strategy across the UK payments industry. The PSB would:

- monitor, report on and make public recommendations to the payments industry;
- be composed of senior industry representatives, senior non-industry representatives (like consumer bodies) and independent directors;
- be overseen by the new Financial Conduct Authority (FCA) which would, at a minimum, set up the Board, make appointments, approve the business plan and budgets and could appoint an independent person to report on its effectiveness; and
- be funded through a levy, set and collected by the FCA.

The Consultation states the aim of this approach being 'to deliver a credible and strong strategy setting public body which would both hold the industry to account and deliver recommendations for the future directions for payments in the UK.' It is proposed the (non-binding) recommendations, addressed to the payments industry, would be accepted and delivered by the Payments Council on the payments industry's behalf.

Option 3 - this would involve the creation of a new regulator for the payments industry, similar to the body 'Paycom' recommended by the Cruikshank Report all the way back in 2000. It would function in a similar way to regulators for utility providers with providers being licensed and the regulator enforcing licence conditions to ensure that:

- open access to payments

systems was maintained;
- pricing was transparent and efficient;
- industry governance was adequate; and
- fair trading principles were respected.

This would clearly result in a significant increase in the overall regulatory burden with considerable costs for businesses attached.

Food for thought

One of the most interesting aspects of the Consultation is the trigger i.e. the cheques decision. Many would argue that the Payments Council's decision to set an end date for cheques of 2018 was not necessarily the wrong decision (it would, for example, have obliged the larger institutions to commit to innovating and educating to meet the deadline), rather the decision was arrived at and communicated in the wrong way. The trigger has therefore highlighted to the payments industry the importance of politics in setting strategy in today's world and how the failure to take into account (and react to) external views can have serious implications. The message seems to be that institutional 'cosiness' (whether perceived or real) is not acceptable and the payments industry needs to be more in touch with the 'real world'. The payments industry no doubt recognises this and acknowledges some kind of change is required - there is clearly no 'do nothing' option.

Whether HM Treasury's preferred Option 2 would achieve the Consultation's stated aims and really drive payments strategy forward is another matter. The creation of a PSB would likely be welcomed by industry and other stakeholders alike, but its spin-off into the void, disconnected from the industry, may not be as welcome, due to the risk of fragmentation (and therefore costs) this could bring. An already overstretched FCA may also be concerned about any proposed increase in its supervisory burden.

The creation of a PSB would likely be welcomed by industry and other stakeholders alike, but its spin-off into the void, disconnected from the industry, may not be as welcome, due to the risk of fragmentation (and therefore costs) this could bring.

One option not considered by the Consultation which would perhaps find more favour within the industry and the FCA would be something of a hybrid between Option 1 and Option 2, whereby a separate body (the PSB), possibly lightly regulated, is created to set strategy and drive this forward (Option 2) but this body forms part of the Payments Council (Option 1). The Payments Council would in turn be reformed to broaden its scope and activities, and the PSB would have powers to mandate the implementation of the strategy set (assuming appropriate consultation and cost/benefit analysis has been performed). Reform of the Payments Council could include modifying the Board structure and membership criteria to create greater balance of stakeholder representation; broadening of scope to draw in card schemes, mobile network operators, technology providers and other 'new generation' payment service providers. The result of this hybrid could be likened to the relationship between the London 2012 Organising Committee of the Olympic Games and Paralympic Games who were responsible for preparing and staging the London 2012 Games, and the Olympic Delivery Authority, the body responsible for developing and building the new venues and infrastructure for the Games and their use after 2012. The PSB would be separately identifiable and solely responsible for setting and driving forward payments strategy, separated from the Payments Council from a governance perspective, but structurally integrated and therefore connected with the industry for which it is setting strategy. The Payments Council would then be the delivery body, taking the strategy to implementation.

Of course, there remain many outstanding questions: who would be responsible for setting up the PSB? Who should sit on the PSB? What should regulation (if any) governing the PSB look like? What should any mandatory powers against industry look like and how far should they go? Who will pay for all this? What will happen if there is a change of government? The list goes on. It will be really interesting to see who responds to the Consultation and what views they express. Of particular interest, of course, will be the views of the Payments Council itself which will be most affected by the outcomes.

The Consultation runs from Thursday 19 July to Wednesday 10 October 2012.

Kate Johnson Associate
Osborne Clarke
Kate.Johnson@osborneclarke.com

Statistics on payments and securities trading in the EU

The European Central Bank recently published its annual statistics on cashless payments and payments systems across the European Union. Rita Choudhury, Javier Huerga and Antonio Moreno of the European Central Bank, discuss 2011's statistics and what the numbers tell us about the financial services industry across Europe.

Payment and securities clearing, trading and settlement systems play a pivotal role in a modern economy. The smooth functioning of these systems is a key factor in ensuring a sound currency and is essential to the smooth conduct of monetary policy.

Payments statistics

With a view to enhancing transparency of these systems, the ECB publishes annual statistics that cover cashless payments and payment systems in the European Union (EU) Member States[1], both from an aggregate and country-specific perspective. The latter reflects factors such as the banking structure, business practices and the institutional and legal framework which contribute to differences between national payment habits.

Data is available from 2000 and includes euro area/EU totals and country breakdowns for the following: (i) payment cards, terminals and institutions providing payment services; (ii) cashless payments involving third parties[2], per payment instrument and place of origination; and (iii) transactions through interbank funds transfer systems, encompassing 'retail payment systems' and 'large-value interbank fund transfer systems' (LVPS), collectively the most significant systems in the EU.

Recent developments

The total number of non-cash payments using all types of instruments grew by 5% to €91 billion in 2011 compared with the previous year. Of these, card payments accounted for the majority share (41%) with relatively equal shares contributed by credit transfers (27%) and direct debits (24%). The total value of cashless payments in 2011 was approximately €240 trillion - equivalent to 19 times the EU GDP - representing a growth of 6% from 2010.

The relative importance of each of the main payment instruments continued to vary widely across countries (see Table 1, source ECB). 1. Percentages may not add up to 100% as e-money transactions and other payment instruments are not shown. A dash (-) indicates data is not applicable. 2. In the case of Luxembourg, a high number of e-money payments are executed on accounts held by non-residents but recorded in Luxembourg due to the methodology applied. Therefore, the relative importance of the payment instruments in Luxembourg appears to be lower than their domestic importance. When disregarding e-money, the relative importance of the main payment instruments in 2011 is: credit transfers (43.84%), direct debits (10.63%), cards (45.40%) and cheques (0.13%).

At the end of 2011, over 727 million cards with a payment function were in issue in the EU - unchanged on the previous year. While transactions using these cards rose in 2011 by 9% to 37 billion, the average value of around €52 per card transaction was similar to the previous year. At the end of 2011 the number of automated teller machines reached almost half a million, while there were almost 9 million point-of-sale terminals[3] - respective increases of marginally below 1% and of 3% compared to 2010.

Looking to interbank fund transfer systems (IFTS), there are 42 retail payment systems - handling payments of relatively low value and limited time-criticality - which in 2011 accounted for around 40 billion transactions worth €29 trillion. By contrast, LVPS are designed to process urgent or large-value interbank payments. In 2011, there were 15 LVPS, which settled 713 million payments in the EU with a total value of €837 trillion. A high degree of concentration is observed in the activity of IFTS. In 2011, the two main LVPS in the euro area -TARGET2 and EURO1/STEP1 - settled 151 million transactions worth €716 trillion. Meanwhile, CHAPS Sterling in the UK settled over 34 million transactions - worth €74 trillion and 61% of the non-euro area EU market in value terms.

Reporting agents and statistics

Cashless payments are made using a variety of instruments and are cleared and settled in different ways, depending on the national payment systems set up in the various Member States. At end-2011, there were over 8,800 institutions reporting payments statistics - primarily banks or trade associations, but also providers of clearing/settlement infrastructures and other institutions offering payment services as defined by the Payment Services Directive (PSD)[4]. This explains some of the difficulties faced in applying harmonised concepts and methodologies to collecting payments and securities data.

Statistics on IFTS cover the participation in payment systems, and transactions by credit institutions and other agents according to a harmonised list of

transaction types. Given that the number of systems is small and the range of transactions in any given system is limited and specified by the rules of the system, these data collection procedures are less complex than those used to gather statistics on cashless payments. The requirements for payments statistics are set out in a guideline[5].

Single Euro Payments Area

Following implementation of the SEPA project[6], all euro payments will be treated as domestic payments so that the current differentiation between national and cross-border payments will disappear. SEPA migration is underway and both national legacy instruments and the new SEPA instruments - credit transfers (SCTs) and direct debits (SDDs) - are being used simultaneously. The ECB is handling developments in the following way:

- In payments statistics, SEPA instruments are currently indistinguishably included in the corresponding items.
- Separate data collection is carried out to monitor the extent of migration to SEPA instruments. These indicators, including the volumes of SCTs/SDDs processed by infrastructures in the euro area, and the share of SCTs/SDDs (in the interbank domain) as a percentage of the total number of transactions processed, are published on the ECB's website[7].

Charts 1 and 2 below illustrate the development of usage of SEPA instruments so far[8]; for example, in July 2012, SCTs accounted for around 30% of all credit transfers in the euro area, while the SDDs' share of all direct debits was 1%.

In the longer-term[9], the ECB plans to expand the reporting framework of payments statistics, through the collection of additional indicators, such as further geographical breakdowns and differentiation of activities of PSPs, to enable the new European payments landscape to be regularly monitored.

Following implementation of the SEPA project, all euro payments will be treated as domestic payments so that the current differentiation between national and cross-border payments will disappear.

Securities

An important component of the financial market[10] is the securities market, activity which needs to be supported by services at each stage of the transaction chain, namely: trade execution, clearance and settlement. As a complement to payments statistics, the ECB publishes statistics on 'securities trading, clearing and settlement' to systems located in the EU.

Securities trading statistics are collected from 31 national and two pan-European securities exchanges which constitute regulated markets within the meaning of the Investment Services Directive[11]. For each securities exchange, four broad groups of indicators are published on: (i) number of participants with access to trading facilities[12]; (ii) number of listed securities; (iii) market capitalisation of listed companies; and (iv) executed trades.

With regard to post-trading infrastructure and processes, securities clearing statistics are collected from 15 central counterparties (CCPs), two of which cover clearing in up to 15 European countries. Information on seven groups of indicators is available: (i) number of clearing members[13]; (ii) non-OTC derivatives contracts cleared; (iii) OTC derivatives contracts cleared; (iv) repurchase transactions cleared; (v) cash transactions cleared; (vi) contracts cleared through a clearing link; and (vii) securities transfers. Numbers and values of transactions are provided, and are broken down by type of instrument and payment.

Securities settlement statistics are collected from 40 central securities depositories[14] (CSDs), including international CSDs. Four key groups of indicators are published: (i) number of participants; (ii) value of securities held on accounts with CSDs, by source and by use; (iii) total number and value of delivery instructions processed, and on an account of a CCP with the CSD; and (iv) number of new issues/redemptions corresponding to securities issued/ safe-kept in the reporting CSD.

Table 2 below shows a list of the seven highest-ranking CSDs, based on the value of delivery instructions processed in the year 2011.

Conclusion

The importance of payment and securities trading, clearing and settlement systems in modern economies has grown considerably over the past decades. Within the EU, and in particular within the euro area, the introduction of the single currency has fostered the integration of these systems. As a result, central banks not only face the task of steering the monetary conditions in the economy, they also have a direct interest in the prudent design and operation of such systems, as reflected in the Statute of the ECB. It is essential that, in their endeavours to promote the soundness and efficiency of these systems, the central banks have comprehensive information at their disposal.

Payments statistics and securities trading, clearing and settlement statistics are published every nine and seven months respectively. Both sets of statistics are accessible in report format[15] or time series[16].

Rita Choudhury Senior Economist
Javier Huerga Principal Economist
Antonio Moreno Principal Economist
European Central Bank
statistics@ecb.int

1. Monthly data is also published on TARGET and other LVPS and on cross-border collateral in Eurosystem credit operations.

2. Third parties, where the payer/beneficiary is not a payment service provider. Currently comprising non-financial corporations; households; non-profit institutions serving households; general government; other financial intermediaries and financial auxiliaries; and insurance corporations and pension funds, excluding MFIs.
3. POS terminal: a device allowing the use of payment cards at a physical point of sale.
4. Directive 2007/64/EC of the European Parliament and of the Council of 13 Nov. 2007 on payment services in the internal market.
5. Guideline of the ECB of 1 August 2007 on monetary, financial institutions and markets statistics (ECB/2007/9).
6. Regulation (EU) No 260/2012 of the European Parliament and of the Council establishing technical and business requirements for credit transfers and direct debits in euro.
7. http://www.ecb.europa.eu/paym/sepa/about/indicators/html/index.en.html
8. SCTs and SDDs schemes were launched in January 2008 and November 2009 respectively.
9. Possibly with effect from 2015 onwards.
10. "Payments, securities and derivatives, and the role of the Eurosystem": http://www.ecb.int/pub/pdf/other/paymentsystem201009en.pdf.
11. Investment Services Directive: http://ec.europa.eu/internal_market/securities/isd/mifid_en.htm
12. Securities trading statistics: four types of participants are central bank, CCP, credit institution or other; two types of location are domestic or non-domestic; type of instrument covers debt, equity and other. Market capitalisation refers only to domestic equities and exclusive foreign listings. For executed trades, system types are electronic order book transactions or negotiated deals.
13. Securities clearing statistics: participants as for securities trading statistics. Three types of location are domestic, non-domestic EU or non-domestic non-EU; type of instrument for derivatives contracts covers financial futures and options, other financial derivatives, commodity options, futures and other derivatives. For repo/cash securities, type of instrument covers debt, equity and other. Breakdown by payment is into euro or other currencies.
14. CSDs: entities which hold and administer securities or other financial assets, hold issuance accounts and enable transactions to be processed by book entry.
15. Payments statistics: http://sdw.ecb.europa.eu/reports.do?node=100000761. Securities statistics: http://sdw.ecb.europa.eu/reports.do?node=1000001578
16. Payments statistics: http://sdw.ecb.europa.eu/browse.do?node=2746; Securities statistics: http://sdw.ecb.europa.eu/browse.do?node=4212911; http://sdw.ecb.europa.eu/browse.do?node=4212912; http://sdw.ecb.europa.eu/browse.do?node=2018796

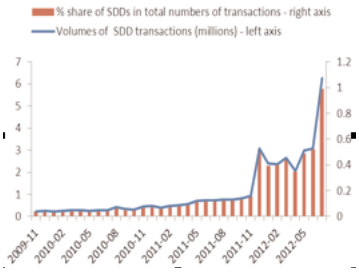
***Table 1**: The relative importance of the main payments instruments in the EU (2011)*

Table 1: Relative importance of the main payment instruments in the EU (2011)

(percentages of total number of transactions[1])

	Credit transfers		Direct debits		Cards		Cheques	
	2011	Change from 2010 (pp)	2011	Change from 2010 (pp)	2011	Change from 2010 (pp)	2011	Change from 2010 (pp)
Belgium	40.99	-1.14	10.58	0.27	46.15	1.44	0.26	-0.04
Bulgaria	72.23	0.57	0.19	-0.07	27.58	-0.50	0.00	-
Czech Republic	55.08	0.45	14.88	-0.80	27.48	4.83	0.07	0.00
Denmark	17.39	-1.02	11.46	-0.48	70.82	1.62	0.33	-0.12
Germany	34.26	0.39	48.73	-1.45	16.58	1.13	0.23	-0.05
Estonia	31.04	-3.19	6.02	-0.65	62.94	3.84	0.00	0.00
Ireland	22.31	-0.31	15.67	-0.03	49.68	1.22	12.33	-0.88
Greece	36.45	2.20	11.42	2.22	39.56	-3.11	10.27	-1.94
Spain	14.67	0.25	39.94	-2.27	43.11	2.29	1.71	-0.14
France	16.98	-0.55	20.15	0.15	45.11	1.77	16.94	-1.36
Italy	30.33	-0.31	14.44	-0.37	37.67	0.15	7.01	-0.87
Cyprus	28.02	0.23	8.22	-0.39	41.58	2.58	21.44	-3.16
Latvia	49.99	-1.94	1.77	-0.12	47.77	2.07	0.01	0.00
Lithuania	55.80	5.31	5.32	-0.80	38.82	-4.49	0.06	-0.02
Luxembourg[2)]	7.43	-2.07	1.80	-0.43	7.69	-1.55	0.02	-0.01
Hungary	63.95	-2.69	7.47	-0.10	27.17	2.78	0.00	0.00
Malta	21.67	1.71	4.18	0.21	43.47	0.99	30.62	-2.97
Netherlands	29.86	-0.39	23.73	-0.43	43.28	0.97	0.00	-
Austria	42.40	0.09	36.86	-0.34	18.89	0.29	0.08	0.00
Poland	60.76	-2.12	0.87	-0.10	38.36	2.22	0.00	0.00
Portugal	11.27	0.66	13.56	-0.21	69.07	1.02	5.95	-1.46
Romania	56.29	-5.48	1.20	0.65	40.46	6.38	2.04	-1.55
Slovenia	49.26	-0.84	15.14	0.20	35.56	0.66	0.04	-0.02
Slovakia	55.18	-0.72	14.52	-0.89	30.28	1.60	0.01	0.00
Finland	46.23	2.85	3.75	-0.48	50.01	-2.37	0.02	0.00
Sweden	27.04	0.92	9.41	0.15	63.54	-1.07	0.01	0.00
United Kingdom	20.24	-0.29	18.67	-0.85	55.64	2.41	5.45	-1.28

***Charts 1 and 2**: The usage of SEPA instruments*



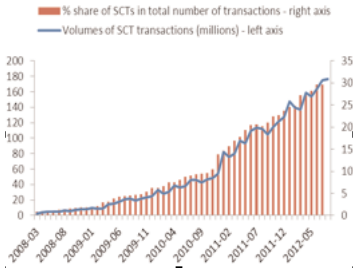


***Table 2**: Delivery instructions processed by the top Central Securities Despositories (2011)*

Table 2: Delivery instructions processed - total for the year 2011

Centralised Securities Depository	€ billions	% EU total
Euroclear Bank (Belgium)	332,959	32
CRESTCo (United Kingdom)	150,178	14
Euroclear France	146,537	14
Iberclear (Spain)	88,199	8
Clearstream Banking Frankfurt (Germany)	80,049	8
Clearstream Banking Luxembourg	74,282	7
Monte Titoli (Italy)	72,160	7
All other systems (31 in total)	50,929	5

New US privacy bill would regulate mobile data collection

The Mobile Device Privacy Act

On 12 September, Representative Ed Markey (D-Mass.) released the 'Mobile Device Privacy Act,'[1] which would require the Federal Trade Commission (FTC) to adopt regulations addressing monitoring software installed on mobile devices. The new obligations would impact wireless service providers, equipment manufacturers, device retailers, operating system providers, website operators, and other online service providers, underscoring the number of industry segments involved and the complexity of addressing privacy concerns in today's mobile wireless ecosystem.

The bill stems from media reports last year regarding Carrier IQ's monitoring software, which was installed on millions of mobile devices. The reports alleged that Carrier IQ's software was tracking keystrokes without user knowledge or permission, spurring a series of lawsuits. "Consumers should be in control of their personal information, including if and when their mobile devices are transmitting data to third parties," said Markey. "This legislation will provide greater transparency into the transmission of consumers' personal information and empower consumers to say no to such transmission."[2]

Under the draft Mobile Device Privacy Act, the FTC would have one year to issue regulations requiring carriers and device retailers to disclose at the point of sale, in a 'clear and conspicuous' manner: (1) The fact that monitoring software is installed; (2) The type of information that the software is capable of collecting and transmitting; (3) The identity of the parties with which the information will be shared; (4) How the information will be used; (5) The procedures by which a consumer who has consented to the collection and transmission of information by monitoring software may exercise the opportunity to prohibit further collection and transmission; and (6) Further information the FTC may 'consider appropriate'.

If the monitoring software is installed after the consumer purchases the device or service, the entity installing the software or providing the software download must make the disclosure. The disclosures must also be displayed (in a clear and conspicuous manner) on the website of the party required to make the disclosures. The Mobile Device Privacy Act authorises the FTC to provide an exemption to the required disclosures if the FTC determines that the use of the monitoring software for a particular purpose is 'consistent with the reasonable expectations of consumers.' Industry groups and privacy advocates are likely to spar over the scope of this exemption.

One noteworthy element of the bill is the definition of 'monitoring software' that spurs a host of new regulations: the term 'monitoring software' means software that has the capability to monitor the usage of a mobile device or the location of the user and to transmit the information collected to another device or system, whether or not such capability is the primary function of the software or the purpose for which the software is marketed. This broad definition would encompass a wide array of mobile apps and services, so much so some industry advocates have expressed concern. For example, Mark MacCarthy, Vice President for Public Policy at the Software & Information Industry Association, commented that the bill 'would impose rigid privacy rules on the mobile industry that can only lead to stagnation and a loss of innovate dynamism.'[3]

The Mobile Device Privacy Act would also require parties to obtain express consent from consumers before the monitoring software begins collecting and transmitting data. In addition, they must provide consumers that have consented with the opportunity at any time to prohibit further collection and transmission of information by such software. The bill would also impose new information security requirements on recipients of the monitoring data. The FTC would have one year to adopt regulations requiring: (1) A security policy addressing the collection, use, sale, other dissemination, and maintenance of the monitoring data; (2) The identification of a point of contact responsible for the management of the security of the information; (3) A process for identifying and assessing 'reasonably foreseeable vulnerabilities' in any system containing monitoring data, which must include regular breach monitoring; (4) A process for preventive and corrective action to mitigate any vulnerabilities identified by the system; (5) A process for disposing monitoring data in a way that makes it 'permanently unreadable or undecipherable'; and (6) A standard method for the destruction of paper documents and other non-electronic data containing such information.

The FTC's regulations require the policies and procedures to be displayed in a clear and conspicuous manner on the recipients' websites. Parties that enter into agreements to share the monitoring data would have to file those agreements with the FTC or the Federal Communications Commission (FCC).

The Markey bill would also establish joint FTC and FCC oversight, with the FCC having enforcement authority over commercial mobile service providers, commercial mobile data service providers, and mobile device manufacturers and the FTC having authority over other parties. The bill also provides for state attorney general suits and a private right of action.

Although the US Presidential election in November makes near-term legislative action unlikely, the bill continues to spark debate between industry groups and consumer advocates over the need for and scope of new data privacy and security legislation.

Mark W. Brennan Associate
Hogan Lovells US LLP
mark.brennan@hoganlovells.com

1. http://markey.house.gov/document/2012/mobile-device-privacy-act-2012
2. http://markey.house.gov/press-release/markey-releases-mobile-device-privacy-act
3. http://www.siia.net/blog/index.php/2012/09/mobile-privacy-time-for-collaboration-not-legislation/

The complexities of online fraud: beyond mere prevention

Online and corporate fraud remains a serious concern for global business and yet part of the problem in tackling the ever evolving nature of fraud comes from the very techniques and approaches used to prevent it. Ian Ross, Principal Consultant at Birzeit Consulting ME, discusses online fraud in its many guises, the problems faced when measuring fraud and the importance of going beyond mere prevention.

The global market research company Frost & Sullivan estimate that there are 2.2 million information security professionals worldwide. This figure is expected to increase to nearly 4.2 million by 2015. Naturally security compliance is a must for all companies, companies that form an IT backbone. Consequently, the Information Security industry is going through an exponential growth rate. Current worldwide growth rate is billed at 21%. The information security industry is currently over $100 billion ($60 B in US, $20B UK, $4.5 B Japan, over $1.5 B in India).

So acknowledgement and 'credit' where it is due, must go to the financial institutions for the marked increase in fraud prevention controls over the past three years, especially formulated to grow with the surge in popularity of social media, e-commerce, and mobile services. E-finance is proof of the benefits consumers are enjoying from information and communication technologies. But there is also the creation of a worthless fraud prevention sub-market: 'solutions' based IT resources, a means of leeching off the need for security and fraud prevention.

These same technologies can cause harm, when personal consumer information is stolen by way of fraud and identity theft. Studies show that information systems workers, as expert as they are in matters technical and analytical, lack basic security knowledge. Since 2005, an estimated 543 million records have been lost globally from over 2,800 data breaches, and identity theft caused $13.3 billion in consumer financial loss in 2011 (BJS, 2011). Thus it is a major challenge for policy makers whose job is to keep on the right side of the law while trying not to lose the business, by balancing ex-ante regulation with ex-post litigation to protect both consumer and commercial interests.

Furthermore, a survey among lawyers in the USA, UK and Europe shows a serious concern about Cloud Computing Services. Data in the cloud is a business risk, but when we look beyond the business risk, there emanates a conflict, which in turn equals risk of loss to fraud and puts companies at risk of massive penalties because of 'naturally occurring' data protection transgressions. Legal experts contacted by 'Future Intelligence' (independent IT analysts) say that in its current state, the cloud technology system worth £14.4 billion globally to the technology companies promoting it puts companies trusting personal data in breach of data protection legislation. Legal experts have also uncovered the potential for corporate fraud. The natural cross-over opens the can of worms, which squirm off in different directions: data fraud, breaches of auditing standards, financial statement fraud, 'skimming' or understated sales or debtor payments.

Therefore, getting behind enemy lines, as opposed to following never ending sales-lines may warrant some thought. The battle-plans drawn up by fraudsters vary as much as the countries in which they operate, some with single-cause fraud motives, or those who attack with a scatter of scams, cyber-attacks and multi-layered, organised and systemically networked financial crime activity. Online fraud will come into play at either one or at all of the stages of the activity, especially when extensive money laundering is concerned. The crux of the matter is the side-line involvement with worldwide business pursuits, such as betting, (online fraud certainly included) gambling, sports (complete with match-fixing) over to car dealerships, real estate et al. One hub feeds out to many lines and outlets of money laundering or specific fraud or corruption. Other organisations as we know run their money laundering and fraud as an ingredient through their own business lines; subtly disguised and 'tweaked' to suit them and resist investigation.

A trillion-dollar war

By some estimates, the war on drugs in the USA alone has cost close to a trillion dollars. According to the government's latest 'Survey on Drug Use and Health,' more than 22 million Americans - nearly 9% of the US population - used illegal drugs in 2010. Is there an inescapable link to fraud in order to fund drug habits? Afraid so. Many criminals have gone beyond shoplifting to do this and say 'ID theft is the way to go'. And laundering drug money is often done online and via social networks.

Hence, the amounts of money involved are immeasurable. So where are the systems and 'controls'? Answer 1: financial institutions cannot agree on what fraud is. The whole concept of

fraud falls down when it gets to the measurement of fraud, private sector regulators insist on creating their own definitions and inconsistent financial fraud measurement parameters. Answer 2: we are spending far too long developing and indulging in recycled initiatives. Yes, we have the Financial Action Task Force (FATF), which rolls out its 'priorities', 'initiatives' and 'recommendations'. Academic research, deeply involved as it is, but with no up-take on converting such projects into workable fraud-fighting resources. A massive void from the woolly strategy to the operational - and not helped by a lack of data sharing and a lack of co-operation with external enforcement resources.

Demonising certain nations as being 'rife' with fraud and corruption, following dubious statistics and dealing in nationalistic stereotyping; has led to a certain way of thinking. That is not to say that massive corruption does not go on in such countries, but commensurate levels of corruption also exist in countries that have a benevolent image (like the UK). Our anti-fraud institutions still insist on working on repetitive partnering initiatives with dated approaches to engaging with stakeholders who carry with them their own political, legal and cultural baggage. This continues locally and globally and keeps us behind the times and behind the criminals. Ironically also (and not just the FATF although they provide the example) in June 2012 the FATF Plenary issued a statement (concerning Turkey), which reviewed the 'voluntary' tax compliance programmes in Curaçao, Spain and Pakistan and issued three reports to outline new trends in money laundering and terrorist financing. Wonderful!

There is no real 'diversion' in dealing with our money launders, or corruption hyenas, so what we are doing in reality is following a 'labelling theory' which drives the anti-fraud initiatives down an aimless avenue.

Hence there is no real 'diversion' in dealing with our money launders, or corruption hyenas, so what we are doing in reality is following a 'labelling theory' which drives the anti-fraud initiatives down an aimless avenue.

Away from specific 'offenders', one colleague in South Africa called for the need to get back to some sound box-standard investigation approaches to fraud. He argues that we have gone too far in relying on technology (and he is the owner of a company that fights cyber-crime by the way!). 'Micro Finance' in the un-banked sector of the population means those people that can least afford it are being forced to pay large sums of money in interest and so the poverty gap increases. Certain countries such as South Africa have a legislated system to control micro-loan companies. This caps the costs; however the rates are still extremely high.

In the USA, seemingly genuine religious organisations, are acting on behalf of criminal groups depositing cash 'donations' into their bank accounts, alleging the funds have been given by worshipers. In another scheme, debit and prepaid cards help money launderers move enormous sums, broken into countless small amounts and of course across international borders without triggering financial controls that monitor larger transactions. A good reason why we should get 'behind enemy lines'.

In Japan, the 'Yakuza' are of course a well-known criminal organisation with a history going back to the 1600s, whose activities do not involve 'street' crime, as this is undignified. Today they are behind the vast cyber-fraud and create more fictitious investment scams than any other country and control 30% of Japan's international financial transactional operations.

Lest we forget those who are meant to be the most assiduous of all - but are not! Police corruption, yielded by fraud and corruption, such as taking bribes, investigative malpractice, and indeed UK tax revenue is someone else's money and not a slush fund for fiddling overtime. In Mexico we have a landmark example of how this is a recognised problem that at last seems to be being taken seriously. The new President Peña Nieto insists he will keep to his mandate of dismantling the 'Ministerial Federal Police' as it became in 2009 (that is until the allegations of buying votes are resolved) as the Federal Investigations Agency was restructured and renamed by the Attorney General's Office, who reported that one-fifth of its officers were under investigation for criminal activity.

We could go on globally; the Russian FSB (which replaced the KGB) is of a construct that enjoys expanded 'responsibilities' but yet has immunity from parliamentary control. Its budgets are never published.

In fighting fraud, we have more facts to contend with than many prefer to acknowledge. No one denies that the human element needs to be controlled by an amount of automation, but when that is taken away we see the total reliance on what is but one means of preventing fraud. In reality, the sheer myriad of fraud schemes and corrupt players creates not just an 'us and them' situation, we have 'us and them and them'! Relying on preventive controls is not enough!

Ian Ross Principal Consultant
Birzeit Consulting ME
iross@bzconsult.com

Turkey's payments industry and the inhibitions to m-payments

Turkey is one of the forerunners of innovative payments technology and openly intends to be a 'cashless society' by 2023. One of the most advanced countries in Europe in terms of countactless mobile payments, Burak Ilgicioglu, a Card & Payment Systems, Business Analysis Manager at Yapi Kredi Bank, Turkey, discusses Turkey's successes so far in regards to mobile payments and the factors hindering widespread adoption.

Turkish banks have a very good history of developing successful card based payment products. All banks have installment products which work mostly as a personal finance product. When people are shopping for a high definition TV, they usually check the campaigns from banks to choose the electronics retailer from installment numbers. There is no finance charges or fees for installment transactions when the customer pays on the due date. All the banks have loyalty programs where customers earn bonus points, just like the frequent flyers programs in the US/UK. This even helps the government fight the shadow economy. Card payments are encouraged by the regulating bodies of the economy. The motto of BKM (the interbank card centre founded by Turkish banks) for 2023 is to reach a 'cashless society' on the 100th anniversary of the republic. Today, 30% of Turkey's total GDP is processed by banking cards.

Turkish banks started the card payment business back in the 80s. BKM was founded in 1990 as the national switch, clearing and settlement processor. Turkey started issuing EMV cards in 1999 and by the end of 2011, the migration was complete. All the ATM and POS terminals now support EMV. All credit cards are EMV with the exception of debit cards; almost all the debit cards are still magnetic stripe. Thanks to Chip&PIN migration which started in 2007, all credit cards are used with offline PIN.

Contactless

Turkey is one of the most advanced countries in Europe in terms of contactless and mobile payments. By the end of Q2 2012, 14 out of 27 banks in the card issuing business have reported that they are issuing contactless cards. More than 6 million contactless cards have already been issued. Turkey is a credit card country, most of these contactless cards are credit cards. There are a limited number of debit and prepaid contactless cards, the majority are credit cards.

Contactless projects started to emerge in Turkey in 2006, when the Chip&PIN migration was still underway. Unlike the US market, Visa and MasterCard forced banks to use EMV for contactless in Europe. This practically means both offline and online transactions are possible due to the contactless interface. This also led to the fast development of NFC products as the natural extension of contactless cards.

Contactless has been gaining momentum in Turkey for the last few years. But just like other countries issuing contactless cards, there are some drawbacks blocking the boom. The main reason is the acceptance infrastructure. There are more than 2 million POS terminals in Turkey and only 60,000 of them have contactless readers installed. It is much lower, when we compare the percentage of contactless cards with the total number of cards, which is 6 million and 51 million respectively. Another obstacle for contactless penetration is that there is not much benefit for both customers and retailers when it comes to contactless. Although some merchants - like Starbucks - are already forwarding customers to the contactless interface to speed up the transaction - there is still a long way to go.

NFC

Despite contactless cards facing issues which have stalled penetration, NFC products have been rolled out in the last two years. We have seen NFC products in different form factors, from Micro SD cards to antenna SIMs

or dongles for iPhone. As for banks, unlike contactless, there is another player on the table, which claims an even bigger share of the customer base: the MNO (mobile network operator). By nature, NFC products work on mobile handsets, especially on SIM cards. As a result, banks and MNOs share the customer.

Currently more than five banks already have commercial NFC products available on different phone and SIM cards. There are three MNOs in Turkey and all of them are actively involved in NFC projects. Current regulations in Turkey require all payment transactions to be processed exclusively through banks, so MNOs are working with many banks at the same time. Almost all the pilot or commercial NFC programs throughout the world feature a single bank and MNO, but in Turkey, all the MNOs have wallets involved with more than one bank at the same time. The physical wallet experience has almost become a reality in the Turkish mobile payment products. Each MNO has already invested in their own TSM (trusted service manager) infrastructure and mobile wallet products. Yet there is still no ISIS-like cooperative organisation between the MNOs and it seems unlikely it will happen in the future.

There are indeed many NFC products commercially available on the market, but the most important player in the game is still missing: the customer. The number of NFC products sold is very low, when compared with traditional card products; there are many reasons for this. We can count the current contactless issues as one. In addition, NFC products require users who have a clear understanding of the personalisation process, which is mostly performed by the customer themselves. Customers are supposed to apply for a card account, install an application to their mobile phone, then authenticate themselves to the payment application on the phone. If everything goes well, then they will surely struggle to find places where contactless cards are accepted. Customer experience has still not been worked out entirely.

Although the current picture doesn't seem to be very promising, there are a great deal of good signs that mobile payments will be the next big thing in Turkey.

Mobile payments

Although the current picture doesn't seem to be very promising, there are a great deal of good signs that mobile payments will be the next big thing in Turkey. All MNOs have dedicated teams for mobile payment services. MNOs are considering mobile payments as part of the mobile wallet product in which people will be utilising location based campaigns, transport ticketing, access control, loyalty card aggregators, couponing and smart posters. For MNOs, it is still more like a loyalty tool, rather than a revenue generator.

Banks are experimenting with mobile payment products. Banks' perception of mobile payment products is not just buying a cup of coffee with the mobile phone. Banks consider the mobile payment experience as a step into the mobile world where the future lays. P2P payments are increasing and banks are positioning themselves in the game. Location based campaigns are another big step for the Turkish banks which already run very successful campaigns for card payments. High value payments over mobile devices will enable banks to penetrate new business models. Money transfers between bank accounts and mobile phone numbers are already a reality in Turkey, yet it will gain another perspective when NFC meets the masses with more prepaid products.

Turkey is definitely a big country for card payments. It will be bigger when the mobile payment experience is part of the daily life and NFC will be the enabler of this evolution.

Burak Ilgicioglu Card & Payment Systems, Business Analysis Manager
Yapi Kredi Bank, Turkey
burak.ilgicioglu@yapikredi.com.tr

Consumer Financial Protection Bureau and remittance transfers

On August 20, the Consumer Financial Protection Bureau released a final rule regarding remittance transfers, amending the rule previously released in February 2012. These new remittance rules are intended to provide greater protections for consumers that transfer money from the United States to foreign countries, and impose a number of significant duties on 'remittance transfer providers,' as Brent Ylvisaker, an Associate at Dorsey, explains.

The Final Rule regarding remittance transfers was passed pursuant to Section 1073 of the Dodd-Frank Act, which amended and expanded the scope of the Electronic Fund Transfer Act ('EFTA'). It marks the first time international money transfers have been comprehensively addressed by federal consumer protection law.

Consumer groups argue the new rules will provide much needed protections for those sending international transfers, particularly immigrants that regularly send funds to their families located in other countries. The Consumer Financial Protection Bureau ('CFPB') Director Richard Cordray has stated that new rules will make 'international money transfers . . . more reliable.' Whether the new rules will actually benefit consumers may be questionable, however. The new rules undeniably provide rules and procedures that are favourable to consumers on the face of it, but the costs of complying with the new rules could turn out to be very significant, especially for smaller remittance transfer providers. These costs of compliance, along with the risks and uncertainty that providers could face due to the Final Rule's error resolution procedures, may reduce the number of providers offering transfers or increase the costs of such transfers. Either a reduction in competition or an increase in price could hurt consumers more than the consumer-friendly rules benefit them.

Scope

The scope of the Final Rule is quite expansive, and appears to include almost all electronic fund transfers made by consumers to overseas recipients. It applies to all electronic transfers of funds 'requested by a sender to a designated recipient that is sent by a remittance transfer provider.' A 'remittance transfer provider' is defined as 'any person that provides remittance transfers for a consumer in the normal course of its business regardless of whether the consumer holds an account with such person.' Remittance transfers covered by the rule include electronic transfers of funds being sent to a specifically identified recipient that were specifically requested by a US consumer requesting the transfer primarily for personal, family, or household purposes. Remittance transfers in amounts of $15 or less are exempt from coverage under the Final Rule, as are non-electronic transfer methods such as mailing a check. However, the rule is far-reaching overall. Transfers that would be covered by the Final Rule could include online bill payments and ACH transactions, for example.

UCC preemption

The expansive scope of the Final Rule may have an impact on the scope of other rules. UCC Article 4A currently governs 'funds transfers' processed through a wire service system, but does not apply to any funds transfer governed by EFTA. The Final Rule establishes that wire transfers are governed by EFTA when such wire transfers are also 'remittance transfers,' thus potentially preemption transactions currently governed by Article 4A. Although Article 4A applies primarily to transfers involving large commercial enterprises and dollar amounts, Article 4A does govern some consumer transactions. For these transactions, this preemption will be significant for remittance transfer providers accustomed to operating within Article 4A's preexisting legal framework, as the Final Rule establishes rights,

responsibilities and risk allocation rules different than Article 4A.

Prepaid cards

In certain circumstances, the scope of the Final Rule will include loads or reloads to prepaid cards. This is the case when the issuer of the card being loaded or reloaded sends the card directly to a foreign recipient located at the foreign address, even where the person in the US retains the ability to use the card or withdraw funds. However, if the card is sent by someone other than the issuer, such as a friend or relative of the recipient, the Final Rule would not apply. Thus, although the Final Rule applies to prepaid cards in some circumstances, its scope in this regard is more narrow.

Safe harbour

Initially, the CFPB proposed a safe harbour interpreting the term 'normal course of business' to mean a business that exceeded 25 remittance transfers per year. Though consumer groups supported this 25 transfer threshold, industry commentators argued for thresholds as high as 6,000 transfers per year. The Final Rule establishes a safe harbour threshold of 100 transfers - any business, which made fewer than 100 remittance transfers in the previous calendar year and fewer than 100 in the current calendar year, is not considered to be providing remittance transfers in the normal course of its business. If a company does exceed this 100 transfer threshold, the Final Rule provides a 'reasonable time period' (not to exceed six months) for the business to comply with remittance transfer rules.

Cancellation and refund period

The Final Rule allows remittance transfer senders to cancel

Remittance transfer providers are now required to disclose certain key aspects of a proposed transaction to consumers before the consumer pays for the transfer.

transactions up to 30 minutes after payment has been made - this is reduced from the one-day period provided for previously. Remittance transfers scheduled at least three business days prior to the date of transfer have different cancellation and refund procedures - they can generally be cancelled as long as the cancellation request is received at least three days before the scheduled transfer date.

Prepayment disclosures and receipts

Remittance transfer providers are now required to disclose certain key aspects of a proposed transaction to consumers before the consumer pays for the transfer. These disclosures must be made in English and in any language principally used by the transfer provider in advertising, soliciting or marketing transfer services. Disclosures must generally be in writing that can be retained, but exceptions are allowed for certain circumstances. Prepayment disclosures must disclose: (i) the amount to be transferred to the recipient of funds; (ii) any fees and taxes imposed on the transfer by the remittance provider; (iii) the total amount of the transaction, reflecting any fees and taxes imposed; (iv) the exchange rate; (v) fees and taxes imposed on the transfer by third parties (e.g. foreign governments); (vi) the amount that will be transferred to the recipient if reduced by third party taxes or fees; and (vii) the total amount to be received by the recipient. A receipt must also be provided after payment is made, which contains information provided in prepayment disclosures and offer information such as the customer's error resolution and cancellation rights and the date by which funds will be available to recipients.

Estimate exceptions

The Final Rule does provide certain limited exceptions for the requirement that all disclosed information must be accurate, allowing a remittance transfer provider to provide an estimate of the amount to be received by the recipient rather than an accurate assessment of the actual amount. The first exception is available to insured depository institutions and credit unions that are sending transfers from an account the sender has with the institution, and the institution cannot determine exactly what amounts will be received for 'reasons beyond their control.' This exception is largely meant to apply to remittance transfer providers that operate 'open network' remittances, where the institution has no direct contact or contractual arrangements with entities paying transfer amounts to recipients. It will expire on 21 July 2015. The second exception is available when exact amounts to be received cannot be determined due to the recipient country's laws or the method by which transactions are made in the recipient country. The CFPB has stated its intention to release a list of countries covered by this second exception prior to the effective date of the Final Rule. The third exception is available when transfers are scheduled five or more business days in advance of the transfer.

Error resolution

The Final Rule defines circumstances that would and would not be considered errors. It lays out detailed procedures to be followed in error resolutions, and requires remittance transfer providers to investigate and respond to notices received by senders within 90 days. The Final Rule also establishes a number of rules concerning in what

circumstances a sender or a provider will be considered liable for errors. Perhaps most notably, a remittance transfer provider is strictly liable for incorrect account information provided by remittance transfer senders - this is considered to be an 'error' and the Final Rule would allow senders to resend the transfer or request a refund in such circumstances, even when the provider cannot recover the transferred funds. The Independent Community Bankers of America ('ICBA') has warned that such a rule could encourage 'active fraud and soundness concerns,' a risk that seems obvious and apparent.

Implementation

The Final Rule is set to be implemented on 13 February 2013. This has been met with significant opposition, both from the remittance transfer industry and from within the government. The IBCA has requested the CFPB delay implementation of the Final Rule for a number of reasons, among them that community banks need more time to reach new agreements taking account of the new rules with intermediary institutions and entities. Thirty-two members of Congress wrote a letter to CFPB Director Cordray requesting further studies on the potential impact of the new rules on providers and consumers before the Final Rule is implemented. The CFPB has stated it will work with consumers, industry and regulators in addressing implementation issues.

Costs of compliance

The prepayment disclosure requirements are perhaps the most onerous imposed upon remittance transfer providers by the Final Rule. Requiring providers to provide accurate disclosures of third party taxes and fees arguably necessitates these providers obtaining and monitoring information on intermediary fees and foreign laws - such information gathering may be prohibitively expensive for many providers. Without extensive information, though, upfront and accurate calculations of a remittance transaction's processing costs could be difficult or impossible, and it also could be hard to predict, much less accurately determine, how many institutions and entities a transaction will be rerouted through before reaching the intended recipient. Requirements that exchange rates be disclosed may also necessitate significant research and require providers to manage risk for fluctuating exchange rates. Some industry experts think that the cost of complying with the Final Rule and/or the potential liability risks imposed by it would make it economically unfeasible for many providers to continue providing remittance transfer services.

Conclusion

The Final Rule represents a significant and comprehensive regulation of foreign remittance transfers. New rules regarding the assignment of liability, required disclosures, error resolutions, and rights of cancellation, among others, will likely create significant compliance issues for remittance transfer providers. Although Final Rule may offer more exceptions from coverage than previous iterations of the rules, these exceptions are limited in their scope and at least some are only temporary. As such, providers that will be covered by the Final Rule need to begin working immediately to ensure compliance with the CFPB's new remittance rules. This is especially true given that the CFPB has not demonstrated a great deal of leniency for those they feel are violating consumer protection laws, as demonstrated by the CFPB's recent actions against Capital One and American Express.

Brent Ylvisaker Associate
Dorsey
ylvisaker.brent@dorsey.com