Online and mobile payments:

Supervisory challenges to mitigate security risks

September 2016

Acknowledgements

FinCoNet would like to acknowledge the efforts of Standing Committee 3 in developing and getting this project to finalisation. Standing Committee 3 consists of representatives from Brazil, Canada, China, Japan, Portugal, South Africa and the United Kingdom and had the assistance of staff from the OECD Secretariat. In particular, we would like to thank Maria Lúcia Leitão as Chair of the Standing Committee as well as Teresa Frick, Steve Trites, Takuo Komori, Kensuke Horii, Kazuhito Yoshida, Ikumi Kato,Tiandu Wang, Xiaoxiao Li, Shaoshua Zhang, Stanislaw Zmitrowicz, Andréia Lais de Melo Silva Vargas, Caroline da Silva, Claire Lawrie, Marta Alves, Patrícia Guerra, Carla Ferreira, Inês Póvoa, and Teresa Cutelo, for their work in writing and producing the survey and report.

About FinCoNet

The International Financial Consumer Protection Organisation (FinCoNet) was established in 2003 as an informal network of financial consumer protection regulators and supervisors to discuss consumer protection issues of common interest. It is recognised by the Financial Stability Board (FSB) and Group of 20 (G20).

In November 2013, FinCoNet was formalised as a new international organisation of financial consumer protection supervisory authorities.

The goal of FinCoNet is to promote sound market conduct and enhance financial consumer protection through efficient and effective financial market conduct supervision, with a focus on banking and credit.

FinCoNet members see the Organisation as a valuable forum for sharing information on supervisory tools and best practices for consumer protection regulators in financial services. By sharing best practices and by promoting fair and transparent market practices, FinCoNet aims to strengthen consumer confidence and reduce systemic consumer risk.

Contents

Table of acronyms

App	Application
BIS	Bank for International Settlement
CNP	Card Not Present
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CI	Consumers International
EBA	European Banking Authority
EBPP	Electronic Bill Presentment and Payment
EC	European Commission
ECB	European Central Bank
EMV	Europay, MasterCard, and Visa (standard)
EP	European Parliament
EPC	European Payments Council
EU	European Union
FinCoNet	International Financial Consumer Protection Organisation
FSB	Financial Stability Board
GPFI	Global Partnership for Financial Inclusion
INFE	(OECD) International Network on Financial Education
MNO	Mobile Network Operator
NFC	Near Field Communication
OECD	Organisation for Economic Cooperation and Development
OTP	One-Time Password
PCI DSS	Payment Card Industry Data Security Standard
PSD	(EU) Payment Services Directive
PSP	Payment Service Provider
QR-Code	Quick Response Code
RFID	Radio Frequency Identification
SecuRe Pay	European Forum on the Security of Retail Payments
SEPA	Single Euro Payments Area
SMS	Short Message Service
USSD	Unstructured Supplementary Service Data

EXECUTIVE SUMMARY

Online and mobile payments

The provision of payment services to consumers is going through a period of rapid change driven by technological innovation. Ensuring consumers' interests are protected when making payments through these new and emerging delivery channels presents a major challenge to supervisory authorities.

New services and delivery channels offer many potential **benefits** to consumers, such as access to payment services in an easier, quicker and more convenient manner, and sometimes at a lower price, allowing also consumers to make cross-border transactions with payment service providers (PSPs) not established in their jurisdiction. Digital payment services available have increased in number and currently offer a greater choice of features across the world.[1] In developed economies, new generations are motivated to quickly adopt new digital payment services. The development of electronic commerce also explains the increasing use of these payments. In developing countries, digital payment services are a key instrument for financial inclusion, and mobile devices are an important tool for cross-border flows of funds (remittances).

However, the various components of payment services are not standardised and there are no itemised and statistical data on the digital payment services available, and their acceptance. Moreover, digital payment services are regularly associated with a specific provider, which prevents their categorisation. The number and diversity of PSPs has increased in recent years, and their activity targets the online and mobile payments markets. The importance of non-financial providers in the digital payments market has also increased. The lack of a categorisation, statistical data, and the provision of payment services by different players may hamper a comprehensive and thorough knowledge of the market and may compromise the issue of international guidance.

Online and mobile payments also present **risks** to consumers, in particular regarding security. Fraud, deceptive practices and lack of reliability of devices and infrastructures are the main security incidents. Transparency of charges and disclosure of information are also challenging supervisors, from a consumer protection perspective.

FinCoNet members identified the issue of security risks as an important threat to consumer protection, which required detailed examination. Thus, a working group (Standing Committee 3) was set up to study the supervisory approaches adopted in overseeing online and mobile payment services and providers, to promote reflection among supervisors, and to share findings and examples of actions to be adopted by conduct of business supervisors.

This report is the result of the work undertaken by Standing Committee 3. It is based on the assessment of the responses given by national supervisory authorities to the *'FinCoNet Survey on*

[1] Virtual currencies are outside of the scope of this report; it only takes into consideration electronic money payments. For the purpose of this report, 'digital' refers to both online and mobile.

online and mobile payments: supervisory challenges to mitigate security risks' (the 'survey'). The analysis of the responses was complemented by desk-based research.

Purpose and overview of the report

This Report aims:

(i) to bring together results of research and survey responses regarding the regulatory and supervisory approaches used to tackle the challenges that digital payments present to the traditional consumer protection framework;
(ii) to inform supervisory authorities of main emerging issues;
(iii) to contribute to the assessment of regulatory and supervisory approaches that have been adopted at national level; and
(iv) to identify good practices being developed by international *fora*.

The study focuses on how regulators and supervisors are responding to emerging risks, particularly security risks, and are keeping up with the pace of innovation, and on issues to be addressed in order to increase consumer trust and confidence in new digital payment systems.

To consolidate the analysis, the report identifies and sets out the next steps for the progress of further work to be developed on the subject.

The report is organised in seven chapters that address the following topics:

- Background analysis of the new paradigm of payment services, the drivers of its growth, the main obstacles to its widespread use and its importance in the agenda of international *fora*.
- Description of the key innovative payment services in online and mobile platforms reported by the respondents;
- Identification of the PSPs operating in the various jurisdictions, namely traditional providers and new types of providers;
- Analysis of the major security risks, and their main drivers;
- Description of the regulatory frameworks in place for online and mobile payment services as well international guidance and self-regulation initiatives;
- Reflection on the supervisory perimeter of online and mobile PSPs, and the effectiveness and efficiency of identified supervisory tools to tackle security risks raised by digital payments;
- The importance of international cooperation with relevant *fora* and overall conclusions.

Overview of the survey

The analysis carried out is based on the responses to the survey and complemented by desk-based research.[2] The survey was sent at the end of April 2015 to collect information on online and mobile payment services and instruments, on payment providers, and on the regulatory and supervisory frameworks applicable. The survey reached a significant number of regulatory and/or supervisory competent authorities in various jurisdictions as well as representative bodies across the world, including all FinCoNet members.

The following topics were addressed in the survey:

- Topic 1. *'Payment instruments and related services on online and mobile platforms'*, to gather data on the payment instruments and related services available on online and mobile platforms, and their key innovative features.
- Topic 2. '*Providers of online and mobile payments'*, to collect information on providers acting on the innovative types of payments and their characteristics.
- Topic 3. '*Security risks of online and mobile payments'*, to collect information on the security risks related to the services and to the providers of online and mobile payments.
- Topic 4. '*Regulatory and supervisory framework for online and mobile payments'*, to access information on the competent authorities, on the characteristics of the regulatory and supervisory frameworks, and on the financial education initiatives.

The Standing Committee 3 was pleased to receive the important contribution of 27 responses from different jurisdictions, covering all continents;[3] 16 responses were from FinCoNet members and 11 from other countries.[4]

Next steps proposal

Taking as a basis the survey and desk-based research, FinCoNet has identified a number of **areas for further work** on online and mobile payments to enable supervisory authorities to deal with various risks:

- **Standardising the categorisation of online and mobile payment services**, aiming at a comprehensive understanding of the ever evolving payments market.

  In order to achieve an accurate and globally recognised categorisation, FinCoNet presents its tentative breakdown proposal of digital payment services to the relevant national stakeholders

[2] The responses to the survey were collected using the cut-off date of mid-December.
[3] See the list of the respondent jurisdictions in appendix.
[4] In this report, 'jurisdiction' refers to one of the jurisdictions that responded to the survey.

and other international *fora.*[5] FinCoNet intends to promote bilateral contacts with specialised international organisations, such as EBA, World Bank, OECD, and GPFI, to collect their perspective and views about the categorisation proposed in this report. Moreover, FinCoNet encourages all members to promote a national discussion among supervisors, payment systems overseers and other relevant entities about the proposed categorisation of digital payment services and the subsequent communication of the conclusions reached to FinCoNet.

- **Collecting statistical data** and other relevant information on the development and use of innovative payment services and the most frequent security incidents at domestic and international level, shedding light on the diversity of these services' innovative features, the risks involved and their causal drivers.[6]

  FinCoNet invites its members to develop national surveys based on the proposed categorisation of online and mobile payment services. FinCoNet is willing to collaborate in the analysis of the data collected and promote the dissemination of the information gathered, developing a dynamic and up-to-date platform of information regarding digital payment services.

- **Assessing of the different supervisory frameworks of digital payments** among FinCoNet members in order to identify supervisory approaches regarding online and mobile payments.[7]

  FinCoNet invites its members to gather information on oversight tools to supervise digital payment services' providers and to share it with all members. FinCoNet aims to promote the assessment of the information reported by its members in the comparison table on the FinCoNet's website. FinCoNet encourages its members to collect data not only on security issues, but also on disclosure of information.

Supervisory approach to mitigate security risks

In addition to the proposed areas for further work, FinCoNet has identified conduct of business supervisory challenges regarding the supervision of online and mobile payments. The reflection that FinCoNet is conducting on online and mobile payments and the assessment of the survey responses allow for the presentation of the supervisory approach and examples of actions that conduct of business supervisors may take to mitigate **security risks** raised by digital payments and ensure a more effective conduct of business supervisory approach in this field:

[5] See chapter "Online and mobile payment services" of this report; a breakdown is proposed of digital payment services under the two main categories of online and mobile payments which should be considered.
[6] See chapters "Online and mobile payment services" and "Security risks".
[7] See chapters "Regulatory framework" and "Supervisory framework".

Conduct of business supervisory challenges	Supervisory approach	Examples of actions to be taken
• **Ongoing and comprehensive monitoring of the innovative payment services market, the main risks and specifications of the channels used, and the assessment of the market share of digital payments**	• When monitoring the payments market, supervisors may assess the development of digital payments and the main security incidents, thus splitting payments by channel	• Surveys addressed to PSPs and/or to users • Mandatory reports of PSPs • Exchange of information among national supervisory authorities (financial and non-financial sector)
• **Close cooperation between conduct of business supervisors, prudential supervisors, payment systems overseers and other relevant entities at the domestic and international level, aimed at continuous information sharing regarding security incidents and risk mitigation initiatives**	• Encouragement of multidisciplinary groups − made up of prudential supervisors, payment systems overseers and other relevant entities − to discuss security incidents and action to mitigate security risks	• Multidisciplinary formal group (set up or) led by the Government • Informal platform for exchange of information • International dialogue and cooperation among supervisors, overseers and other relevant entities
• **Close supervision of online and mobile PSPs to ensure the implementation and adoption of rules leading to the disclosure of the features of each payment service, the specific risks arising and the safety procedures available for adoption by the user in relation to each payment transaction**	• Supervisors may oversee PSPs' disclosure of information to users on the risks and security procedures each time a user accesses any payment service	• Off-site monitoring of PSPs' websites, home banking, apps, and other digital channels to assess compliance with mandatory requirements on the disclosure of risk and precautionary attitudes • Pre-approval of a Key Information Document (KID) regarding a specific payment service
• **Ongoing assessment of security risks through the use of a variety of supervisory tools, particularly in respect of the management of complaints, to identify the most frequent and new security risks and their importance for consumer protection, allowing supervisors to promote targeted actions**	• Analysis of collected data to identify the most significant security incidents and PSPs involved in order to take supervisory action to prevent and mitigate security risks • Information sharing with prudential supervisors regarding security concerns where relevant	• Analysis of information provided by the complaints management system, on-site inspections and off-site monitoring • Propose new regulations to offset regulatory gaps identified through supervisory tools

Conduct of business supervisory challenges	Supervisory approach	Examples of actions to be taken
which could include the identification of regulatory gaps		
• **Promotion of awareness campaigns on risks raised by digital payments, specifically regarding emerging security risks or major security incidents**	• Supervisors may include in their mandate the launching of awareness campaigns on users' need to comply with security procedures and requirements that promote a balance between convenience and security • Supervisors may include in their mandate the regular publication of information on features and risks regarding new digital payment services through booklets, flyers and online (website)	• Awareness campaigns focused on the risks raised by innovative payment services and security precautions that users should follow • Definition of contents on conduct of business supervisors' websites regarding security issues related to online and mobile payment services
• **Coordinated approach between conduct of business supervisors and national bodies responsible for financial literacy to promote the use of precautionary procedures by digital customers**	• Supervisors may maintain close collaboration with financial literacy bodies to further promote precautionary attitudes and safety procedures by users, enhancing the impact and the dissemination of supervision-based information	• Financial literacy bodies may disseminate information on the features and risks of new digital payment services based on information provided by financial supervisors • Financial literacy bodies may address the new risks associated with digital channels and run initiatives to promote precautionary attitudes by users (e.g. strong customer authentication)

BACKGROUND

Traditional payments can now be carried out through online and mobile channels. The growth of online and mobile payment services, driven by technological innovation and supported by new users' behaviour and financial inclusion, brings advantages to consumers as well as new challenges to financial supervisors. The ongoing technological developments allow the emergence of new PSPs, who respond to users' expectations for faster, efficient, convenient, and, hopefully, more secure services.

Online payments can be defined as payments whose initiation order is placed on devices connected to the internet (namely, desktop PCs, laptops, tablets and mobile phones), with payment instructions also given, and confirmed, online, between customers or merchants and their respective PSPs in an online purchase of goods or services.[8]

Mobile payments include the operations for which payment data and instructions are initiated, transmitted, confirmed and received via a mobile device connected to a mobile communication network, using voice technology, text messaging such as SMS or USSD technology, or contactless radio technologies such as Near Field Communication (NFC) or Bluetooth. The payment operation is made using a keypad or a touch screen (in remote mobile payments) or activating contactless radio technologies (in contactless or proximity mobile payments). Traditional mobile phones, smartphones and other equipment, such as tablets, can be used to access devices for mobile payments.

Payments initiated via the internet using mobile phones (e.g. via mobile banking using a browser on a smartphone) are not considered mobile payments, and are defined as online payments. The same reasoning applies to online payments when the mobile phone is only used for authentication purposes (e.g. by sending a transaction number for online banking transactions via a mobile phone). Likewise, contactless payment cards (using NFC technology) are not considered mobile payments when they are initiated with a payment card. However, if the card chip is embedded in a mobile phone it is considered a mobile payment.[9]

Payments in the digital age

Over the last few years the world has faced a significant digitalisation of daily human activities, influencing the way people communicate and interact with each other through social, commercial and financial relations: "customer relationships used to be human, one-to-one. Then they became remote, one-to-many. Now they are digitised, one-to-one".[10]

Payments that were made face-to-face (e.g. with cash, cards and cheques) are now remotely accessible and can be made through the internet and mobile devices. Digital services have introduced a completely remote payment system, significantly changing consumers' expectations and behaviour. **Technological developments and customers' behaviour** are mutually supportive of each other,

[8] ECB, 2010; BIS, 2012.
[9] ECB, 2010.
[10] Skinner, 2014.

promoting the appearance of new business models and giving customers greater influence over changes in the market.[11]

Currently, consumers need access to everything, everywhere, in conjunction with services more adapted to their convenience. The evolution of technology is responding with the provision of remote financial services, available 24 hours a day and seven days a week.

This is triggered by growing demand by the so-called **Millennials** (or Generation Y) and **Digital Natives** (or Generation Z). The change is inevitable as Millennials grow older and Digital Natives are emerging, becoming decision-makers over financial service providers and forming the majority of the financial consumers.

Millennials and Digital Natives grew up with computers, mobile phones and tablets and, due particularly to the latter, have a greater level of comfort using new technologies. Millennials and Digital Natives are tech-savvy, confident, open-minded and superb multi-taskers, and they want payments made in a fast, easy and satisfactory manner. Their parents and grandparents – the Baby Boomers (or Generation X), continue to value face-to-face relationships and are more likely to use a bank branch service and trust the traditional payment methods.[12] Baby Boomers are inclined to be more concerned about security issues, such as lack of privacy and hacker attacks on their bank accounts.

As Millennials and Digital Natives grow older, one might argue that the days are numbered for the paradigm of going to a bank branch and shaking hands with the account manager. Banking is evolving to suit the needs of those born after 1980, who in 30 years will comprise the bank customer universe.

> *"In the banking space, I'm often confronted with passionate arguments for why face-to-face interactions, the availability of advice and the psychological comfort of brick-and-mortar spaces still matter. The problem is that those describing these "values" are inevitably Baby Boomers or Gen-X consumers, describing their comfort levels and buying behaviours. There are a number of key trends we can observe today that signify an abandonment of this traditional buying behaviour for the next generation of customers".*
>
> *King, 2012*

Behavioural economists speculate on how the easy and clean process of digital payments can be a powerful driver for consumption.[13] They guess that the use of digital payment services, which makes consumption a friendlier experience than using cash, can influence people's spending behaviour. Therefore, it can stimulate consumption and the use of credit and, consequently, may jeopardise the principle of responsible consumption and the principle of responsible credit. This is a reason for concern and an issue that supervisors should monitor with interest.

Nevertheless, the emergence of digital solutions in the payment services market is coming along with **new financial tools**, such as apps that limit choices and allow consumers to check their account balances prior to making purchases or even to programme the mobile phone to block any payment

[11] Hayashi, 2012.
[12] Krishnan, 2014.
[13] Thaler, 2015.

above a daily set amount, and to receive warnings when expenses reach a chosen threshold for different categories of spending, thereby preventing users from falling into temptation.

> *"If more payments move to phones, we will need to be ever more aware of the way our brains work when making purchases. A smartphone is an additional step removed from cash, after all. At least people who have had bad experiences with debt or identity theft might recall those things each time they pull out a plastic payment card. Not so with a shiny iPhone and Apple Pay.*
>
> *What would really be useful is some kind of physical reminder, an app of some sort that turns itself on when it senses that a phone payment is about to happen. A little jolt of electricity would be nice, just to deliver the same kind of vivid feeling that we used to get once upon a time when parting with our hard-earned paper money".*
>
> *Lieber, 2014*

In fact, there is currently a multiplicity of sophisticated financial apps that can also be used as tools for better financial management, and which may be combined with a payment device, e.g. apps that install non-fungible budgets to help users make a serious effort to create a financial plan. These "buckets and budgets" aimed at assisting users in assuring that they live within their means can lead to better decision-making on how much should be spent on food, housing, transport or leisure.[14] When associated with the mobile payment app, they easily inform the user how much was spent on a specific store, goods, and category of product or service.

In this way, these new tools could help consumers with their own **money management**. This could be especially useful for Millennials, who have a greater appetite for immediate rewards, and for whom the opportunity to obtain immediate gratification may compromise their money management skills, as it was also remarked by behavioural analysis.

Another key point is the fact that digital payments have gained significant importance for **financial inclusion.** The new system, which does not necessarily depend on bank branches, provides a freedom of action whereby more people can access the financial market and, in particular, the payment system. Mobile technologies have made an important contribution to increase access to financial services by **underserved populations**[15] and to a greater extend by the **unbanked and under-banked population**, particularly relevant in developing countries, where in some cases the number of adults using mobile money accounts is higher than those using traditional bank accounts.[16] Digital payments are playing a pivotal role in progressing towards universal access to financial services. Shifting transfers and wages digitally into accounts represents an enormous opportunity for making payments more convenient and increasing the use of accounts in developing economies.[17] Digital payments also support international remittances especially important to the economy of undeveloped countries.

Moreover, the advantages of online and mobile payments **for merchants** are also noteworthy, especially in relation to the **cost reduction** in processing operations when compared with traditional

[14] Thaler, 2015.
[15] FED, 2015.
[16] EP, 2015.
[17] World Bank, 2015.

payment services. The processing of digital payments is generally less onerous than that of traditional payment orders, which are processed manually and/or on paper, and whose costs are higher when processing large sets of data. Furthermore, mobile payments are usually an easy experience, thus becoming a strong driver for consumption, a fact that is grasped by merchants who are willing to fully embrace innovations in payments. Mobile payments are frequently a channel for publicity or advertising, and are an opportunity to strengthen the relationship with the consumer and to know the context of the purchase. Additional data on the consumer's habits, such as location, the use of mobile search, other purchases and social networking, give merchants and financial service providers extra knowledge about their customers, and their acquaintances, which in turn may be used to offer them relevant and even personalised products.

"Your mobile identity is fast becoming a combination of your alter ego, your agent and your personal avatar. Your mobile device is becoming a one-stop shopping space for all of your physical and emotional needs".

Krishnan, 2014

"The Internet has made tracking easier, cheaper, and more useful. And clandestine three-letter government agencies are not the only ones spying on us. Amazon monitors our shopping preferences and Google our browsing habits, while Twitter knows what's on our minds. Facebook seems to catch all that information too, along with our social relationships. Mobile operators know not only whom we talk to, but who is nearby".

Mayer-Schönberger and Cukier, 2013

In a nutshell, merchants and providers could take large profit from this new digital era because it gives them the opportunity to reduce costs, to reach more customers and to know them better. Merchants can also diversify points of sale and increase their market share.

The evolution of the online and mobile payments market is unstoppable and it generates significant concerns about the regulatory and supervisory frameworks' ability to deal with these new services, new providers, acting sometimes outside the supervisory perimeter, and new risks on payment services. The innovation process is fast and the regulatory framework needs to keep pace with the developments.

"(...) The rapid development of the internet, the growth of mobile services and other technological innovations have proved highly beneficial to consumers while, at the same time, presenting new challenges, requiring consumer policy makers to not only keep up with developments, but also find ways to address ongoing and emerging issues."

OECD, 2010

Digital payments may become the daily bank account and debit/credit card. This is what supervisors need to be prepared for.

Digital payments in the international agenda

Reports and research published by international policy-making organisations emphasise the considerable relevance of online and mobile payments across the world.[18] While acknowledging and welcoming their importance, they also stress that their potential for growth is limited by some relevant obstacles. Apart from technological barriers, the most important obstacle at the top of the concerns of financial consumer protection organisations is the **security** of the new payment services.

FinCoNet has elected the security issues as a major theme, and would like to contribute to the international reflection about the major challenges it brings to supervision, including the conduct perspective.

One of the technological obstacles to further and faster growth is the **lack of standardisation** of the various components of payment schemes, and interoperability between PSPs.[19] The **lack of interoperability**, including cross-border, between PSPs is also a challenge. Better interoperability would provide consumers with a secure and trusted payment method, while e-shopping, especially in foreign countries, would provide them with more flexible payment options through better switching between different services and providers. This could lead to an increase in the number, speed and volume of internet and mobile transactions.[20]

However, **security issues** are the main obstacles to the use of digital payments. They are referred to as preventing the widespread adoption of e-commerce.[21] Surveys to users also indicate concerns about security as one of the main impediments to the adoption of mobile financial services. [22]

The most significant concern of security requirements is the prevention of **fraud**.[23] According to the European Central Bank, fraudulent activity is now increasingly moving to remote card transactions, in particular to payments over the internet. [24] The majority of the value of fraud has resulted from card not present (CNP), i.e. transactions made without face-to-face contact between the cardholder and the merchant, a tangible payment card to inspect for security features, or a physical signature on a sales draft to check against the card signature; these are the cases of payments made via internet, post or telephone. CNP fraud has grown faster than CNP transactions.

The European Union (EU) also states that, “though innovative technologies offer opportunities to improve customer service and reduce prices, they may also pose regulatory challenges, particularly in relation to cyber-security and data protection”.[25] **Cyber threats** are a major concern for consumers and businesses; this is likely to grow in importance as digitalisation progresses, and requires an appropriate response.

[18] EC, 2012; OECD, 2012b; EC, 2015a.
[19] OECD, 2012b; EP, 2015.
[20] EP, 2015.
[21] EC, 2012; EC, 2015a.
[22] FED, 2015.
[23] EC, 2012; EP, 2015; OECD, 2012a.
[24] ECB, 2015. The European Central Bank analyses the evolution of fraudulent transactions conducted using cards issued within the Single Euro Payments Area (SEPA) and acquired worldwide.
[25] EC, 2015a.

Consumer data protection and **privacy** are issues of concern. Sensitive customer information should stay within a secure payment infrastructure, both in terms of processing and storing data. The number of parties having access to authentication data during or after a payment transaction should be restricted to only those who are needed to perform the transaction.[26]

> *"The biggest fear of corporates and consumers is that transactions will not be processed properly, that their bank access details might be compromised and that their data and therefore their money may be stolen. That is why banks have to step up to a big challenge: guaranteeing data security. The banks of the 21th century need to be bold and guarantee that customer data is secure".*
>
> *"This is why the focus on data and data security is the key to the future".*
>
> *Skinner, 2014*

International organisations also stress that in addition to security issues at the individual level, the potential weaknesses of payment systems in terms of security and reliability could affect the financial system and the economy. Therefore, they raise issues for supervisors concerning their various responsibilities and tasks as catalysts, overseers and/or operators of payment systems.[27]

In addition to the security challenges already identified, **other broad drivers of risk** are mentioned in digital financial inclusion models addressing financial consumer protection. The use of agents as the principal customer interface raises challenges regarding the oversight of the network of agents and introduces increased risks of fraud and theft. The digital technology used may also present certain risks in its own right, as well as additional risks due to the involvement of agents and the profile of the previously financially excluded and underserved customers themselves. Plus, the likelihood that multiple financial providers and non-financial providers' parties will be involved in the storage and management of account data and the holding of customers' funds adds complexity to protecting customers against risk of loss upon the failure of one or more.[28]

Also the EU highlights that **new players** may not always be regulated to the same extent as incumbents by current regulatory and supervisory frameworks, including from a consumer protection perspective. Technological developments and the expansion of new distribution channels may make it difficult to provide appropriate pre-contractual information to customers – for example, by supplying mandatory disclosure via mobile devices with small screens. The appropriate response to these challenges (including adequate security and consumer protection) and opportunities will have to be carefully considered.[29]

The BIS shares the same concern. For regulators, supervisors, and other authorities, a number of issues also arise from the growing presence of non-financial providers in payment systems, especially relating to online and mobile payments. Even if the types of risk do not differ materially between financial and non-financial providers, differences on how they are regulated could translate into differences in risk mitigation measures (and therefore in the probability that risks might materialise and have a potential impact). Some of the issues raised by non-financial players are related to operational

[26] EC, 2012; EP, 2015.
[27] BIS, 2012.
[28] AFI, 2014; CGAP, 2015; G20, 2014.
[29] EC, 2015.

risks, competition issues, and consumer protection aspects (such as, fraud, data privacy and protection of consumers' funds, especially in the event of the non-financial providers' default). Fraudsters are likely to target the points at which data security is weakest, and in this context non-financial providers are probably at a higher risk of data security breach than financial providers.[30]

International organisations underline that overcoming of all these obstacles cannot compromise the maintenance of a proper financial consumer protection framework. They acknowledge that the **level of protection** that consumers have in using different types of payment services varies widely, within countries and from country to country, depending on what mechanisms and channels they use, and the problems they encounter.[31]

Emphasis has been placed on the importance of a **technology-neutral consumer protection framework** that enables consumers in terms of a high level of protection, whatever vehicle they choose to use to make their payments. In particular, consumers should easily have access to full information on the terms and conditions of the contracts, through the disclosure of clear, transparent and complete information. The multiplicity of parties that can be involved in a payment transaction can make it difficult for consumers to understand whom to turn to in case of problems. This is the case, for example, in a mobile payment whose processing involves the mobile device company, the mobile communication service company and the payer and payee's PSP; when such a payment procedure fails, it may not always be clear which party failed.

Greater consumer empowerment and **education initiatives** would be useful in several accounts. First, it would help build awareness on the actions businesses have taken to **ensure security** of online and mobile payments. This in turn would help dispel any misperceptions, as would education aimed at enhancing knowledge of what consumers could do to avoid compromising their financial and personal information. Secondly, consumers need to be knowledgeable about their **rights and responsibilities**. This would help them to make informed decisions, and they would be better prepared to find key information in **disclosure** statements, in particular the fees and charges, and possibly hidden costs. Thirdly, in an e-commerce context, consumers need to understand their rights, but also their responsibilities and the **risks** they bear when making a digital payment. Finally, educated consumers are better equipped to detect and/or **avoid potentially fraudulent and deceptive commercial practices**.[32]

Some international organisations have issued **principles and guidelines** to help shape consumer protection and industry practices. Some of them are generally applicable, regardless of the delivery channel or the technological platform used to perform the transaction. For example, at the request of the G20 Finance Ministers and Central Bank Governors, the **OECD** in collaboration with the **FSB** took the lead in developing *High Level Principles on Financial Consumer Protection*, endorsed by the G20 Leaders in 2011 and as a Recommendation of the OECD in 2012.[33]

Principle 1 on Legal, Regulatory and Supervisory Framework explicitly mentions that financial consumer protection regulation "*should be responsive to new products, designs, technologies and mechanisms*". It adds that *"where relevant, appropriate mechanisms should be developed to address*

[30] BIS, 2014.
[31] OECD, 2012b.
[32] EP, 2015; OECD, 2012b.
[33] OECD, 2011.

new delivery channels for financial services, including through mobile, electronic and branchless distribution of financial services, while preserving their potential benefits for consumers".[34]

The OECD issued updated guidance in 2014[35] to boost consumer protection when using online and mobile payment systems and to identify ways in which policy makers and businesses can work together to strengthen consumer protection, while spurring innovation in the marketplace.[36] It sought to do so in a manner that will remain relevant as the technology used by payment systems evolves. Guidance establishes that consumers should have access to easy-to-use, secure payment mechanisms and to information on the level of security such mechanisms afford. It adds that limitations of liability for unauthorised or fraudulent use of payment systems and chargeback mechanisms offer powerful tools to enhance consumer confidence, and their development and use should be encouraged.

In 2013, the **ECB** published *Recommendations for the security of internet payments* developed by the European Forum on the Security of Retail Payments (SecuRe Pay), which is composed by European supervisors of PSPs and overseers.[37] The overall objective is to foster the establishment of a harmonised EU/European Economic Area-wide minimum level of security. The 14 Recommendations are organised in three categories: (1) general control and security environment of the platform supporting the internet payment service; (2) specific control and security measures for internet payments; and (3) customer awareness, education and communication. Some good practices, which PSPs, governance authorities of payment schemes and other market participants are encouraged to adopt, are also presented.

The members of the Forum are committed to supporting the implementation of the Recommendations in their respective jurisdictions, and will integrate them into existing supervisory/oversight frameworks. In 2014, the ECB published a guide for assessing country compliance with the Recommendations. These Recommendations were converted into **EBA** Guidelines in 2014, with the objective of providing a solid legal basis for the consistent implementation of the requirements across the 28 EU Member States. They are applicable as of 1 August 2015.[38]

Guidance about security in digital payments comes from a different range of international organisations. This reflection is being developed not only from the consumer protection point of view, but also taking into consideration the consequences of the lack of reliability and trust in the financial system, which shows that the mitigation of risks raised by online and mobile payments implies a widespread cooperation.

[34] OECD, 2011.
[35] The initial *OECD Guidelines for Consumer Protection in the Context of Electronic Commerce* were adopted in 1999, http://www.oecd.org/sti/consumer/34023811.pdf
[36] OECD, 2014.
[37] ECB, 2013a. In the same, the ECB also published a public consultation of *Recommendations for the security mobile payments* (ECB, 2013b).
[38] EBA, 2014.

ONLINE AND MOBILE PAYMENT SERVICES

Key points from the survey responses

- There is a wide range of online and mobile payment services, and their features are diversified among jurisdictions due to different levels of economic and financial development as well as available infrastructures.
- Most new digital payment services are tied to specific providers and labels, making it difficult to group services by standardised categories.
- Data about the digital payment services available on the market and their acceptance by consumers and merchants are not widely available, hampering a comprehensive and in-depth knowledge of the market and its evolution.
- Online and mobile payment services are usually available cross border – although mobile payment services are more often available only at national level – calling for international guidance.
- The growth of digital payment services is hindered by some barriers, regarding customers' security concerns and attitudes, the associated costs and the complexity of systems' features when compared with cash.

Overview

The last few decades have brought about the digitalisation of banking services, in particular of payment services. The beginning of the digital era in payment services was marked by the home banking service and the acceptance of (physical) credit card identification numbers to make purchases on the internet. The evolution of online services generated virtual card services and prepaid electronic money accounts, segregating physical from digital payment instruments.

The wide dissemination of the internet, in particular wireless internet, and mobile devices with mobile internet access (smartphones) is strongly contributing to the development of innovative payment services and instruments in online and mobile platforms.

The technical developments in devices and infrastructures and the higher penetration of mobile devices are among the fundamental drivers of innovation in digital payment services. Its widespread use is still limited by several barriers.

The diversity of online and mobile payment services, the multiplicity and combination of innovative features and the various possible national perspectives hinder the definition of a single, homogeneous and stable categorisation of digital payment services. Considering that digital payments are relatively recent and constantly evolving, standard definitions and a common classification have not yet been adopted. And when adopted they should be dynamic to permanently reflect the evolution of the market.

The adoption of an interim classification is actually a difficult task. The responses to the survey led to the conclusion that the information regarding the categorisation of the different new payment services

and their pace of growth is still scarce and the relative market share of digital payments unknown. Many jurisdictions have stated that detailed information is not available, and many reported that the information available is mainly related to the general use of online and mobile services, showing that data by type of service are missing.

Categorisation of payment services

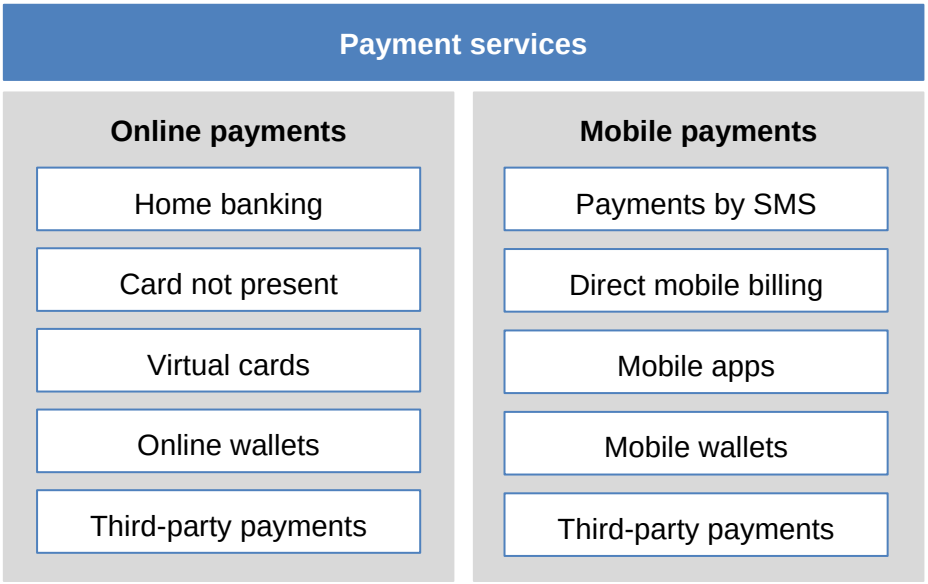
The analysis of the survey responses indicates that there is a wide range of online and mobile payment services, incorporating diverse innovative features, often related to specific national needs and realities. Responses also indicate that these new payment services are often associated with traditional payment services or instruments, such as payment cards, direct debits, credit transfers, money remittances and cash-in-cash-out operations. The innovative features are mainly the channels through which people use those services and instruments.

The technological features embedded in the digital payment services are frequently a hybrid result of online and mobile functionalities looking for a boost in efficiency and ease of use for consumers, thus resulting in the popularity of those services in the market. Many of the online and mobile payment services reported by respondent jurisdictions are also incorporating new features focused on the improvement of security measures, aiming to enhance the confidence of consumers and merchants in the new payment services.

The analysis of the survey responses also draws the conclusion that many of the new digital payment services available are associated with a specific payment provider, with unique features and use limited to particular situations or stores.

Moreover, the responses to the survey suggest that innovations in online and mobile payment services were initially developed to target the domestic market. However, similar innovative features emerged in different countries worldwide, with some minor differences related to domestic market conditions.

The specificities found in the information gathered from the survey responses show that a classification of online and mobile payment services in categories is a challenging task. Considering the responses received and a desk-based research, this report presents a tentative breakdown of digital payment services under the two main categories of online and mobile payments. Different types of services fall within each of these categories according to their primary attributes and features.



Online payments

The services delivered by financial institutions on their websites, through home banking services, have improved and currently allow customers to order payments at any time. Virtual cards and virtual wallets facilitate online payments, especially for those who avoid home banking services. Online stores developed their systems to include payment services for their customers. Third-party payments processing initiation also provide payment channels in which customers do not need to disclose personal data to various web merchants.

Referring to the survey responses obtained, all respondents indicated the existence of online payment services. There are, however, differences among countries in terms of national market developments.

Home banking

Home banking comprises a set of banking services (such as checking account balance, viewing bank statements, order credit transfers and order payment transactions) accessible through the internet. In the survey, home banking was identified by a large group of respondents as being provided by various deposit and credit institutions. It is available worldwide and is largely used by customers.

Home banking is not only available through online platforms but also through mobile devices with access to the internet (commonly referred to as mobile banking services). The payment services available are various: credit transfer, money remittance, transfer of funds to payment accounts, payment of bills, payments to the State, and management of direct debit operations, among others.

Customers rely on the home banking service, although it may be subject to scam attacks through the theft of access credentials and fraudulent access to bank accounts. Banks worldwide have been investing in more sophisticated security systems, imposing stronger levels of authentication for their customers. A large number of credit institutions have already implemented a two-level authentication: the first level is the home banking access to the bank's website, usually with a username and password (which can be a full password or a request of random digit positions); the second level

requests a dynamic code or OTP (an SMS token code, a hard token code, or a matrix card reference). Some mobile banking services may use biometric readers for authentication.

Card-not-present payments

Card-not-present (CNP) payments are payment transactions in which the merchant does not have access to the physical payment card to process the payment order. They are common in e-commerce payments over the internet using the details of a physical payment card. In this service, customers shopping on websites have to provide merchants with their payment card number and the security codes to finalise the payment.

This service has a significant security risk, as the payment card details may be given to merchants with scarce or no security measures implemented, and consequently data may be hacked and used fraudulently. To accomplish a higher level of security, some card schemes have been investing in extra security measures in order to increase customers' confidence in these means of payment.

In addition to their use for online payments, the majority of payment cards in Europe and Australia currently include NFC technology, which allows contactless payments at the point of sale.

Virtual cards

The virtual card is a card-based payment service where a replica temporary card number with a reduced validity period, limited usage and a pre-defined spending limit is generated to be used for internet purchases.[39] These cards may be proxies for physical debit or credit cards owned by the payer, allowing web payments without disclosing the details of the physical payment card. Besides payments to merchants, virtual cards also allow person-to-person transfers.

The details for the virtual payment card can be provided on a webpage or received by SMS on the user's mobile phone.

Virtual cards are considered safer than card not present, as customers avoid the disclosure of personal and financial data to various e-merchants. Potential risk of fraud is also reduced because virtual cards may have a very short expiration date and small spending limits.

Virtual cards may be issued by financial providers (such as deposit and credit institutions), but also by other non-financial payment providers.

In 2001, in Portugal, the national payment processor company developed, in close cooperation with national banks, an option for the user whereby a temporary virtual payment card is created to use in online transactions. This payment service requires previous enrolment of the user's physical payment card, either via a dedicated function in the ATM network or via the home banking facilities of participating issuers. After the enrolment, the user can generate a virtual card for a given online transaction, in a dedicated website. When enrolling the card, the user may set amount limits per day and per each individual virtual card. Another option given to the user allows for the generation of a virtual payment card valid for up to one year, but only for a specific e-merchant. This online payment service has had high acceptance in Portugal.

[39] EBA, 2014.

Online wallets

Online wallets are a set of procedures agreed between a wallet provider and a consumer to initiate payments from linked payment cards or checked accounts. Online wallet services are usually linked to one or more payment instruments and allow customers to make payments to several e-merchants.[40]

To create a virtual wallet, the user must register with a payment provider and the wallet is usually linked to the user's email address.[41] The user can then upload money into the account, generally using a debit or credit card or making credit transfers from her/his deposit account. The electronic money stored in the online wallet is a digital equivalent of cash. Payments are authorised after entering username and password. These procedures allow the customer to purchase online in a simpler and safer way.

Online wallets may be incorporated in online banking tools made available to consumers by their deposit and credit institutions, or offered by a third party, such as merchants associations. Furthermore, they may allow both the customer and the merchant to benefit from other services, such as loyalty programmes or other marketing actions.

Third party payment initiation

There are several online payment systems intermediating payments between customers and merchants. Merchants have to sign up for the service with the processor, and customers usually have to register a service account with the processor and associate a bank account or payment card. The payment is then executed by the processor through its own platform or by enabling consumers to pay online through their bank's website.

These services give customers a safer platform to make payments, as their personal data are only given to the processor and not to several merchants.

This online payment service is usually based on financial providers (such as banks), who act as third PSPs, because they make payments on behalf of their customers, initiating payment transactions. In the Netherlands, one of the most commonly used online payment methods is a third party payment provider platform developed by Dutch banks.

Non-financial entities may also provide these services, as is the case, for example, of the Australian Post.

[40] EBA, 2014.
[41] OECD, 2012b.

Mobile payments

Mobile payment services allow customers to make payments anywhere. Through a mobile device, customers have access to services adapted to their specific needs, to be used with a single merchant or different traders, using varied technologies, such as SMS or via NFC for remote or local payments.

Contrary to the responses regarding online payment services, a few survey respondents reported not having mobile payment services available locally. This is the case, for example, of Saudi Arabia or Chile.

Payments by SMS

There are payment services based on text messages sent by the payer through a mobile device. The payer has to indicate the beneficiary and the amount, which is directly charged to the phone bill. This service is not restricted to smartphones, and is also available on traditional mobile phones, thus contributing to a potentially wider use of mobile payment services. Among the survey responses, this type of payment service was mentioned, for example, by Australia, Austria and Indonesia.

Direct mobile billing

Direct mobile billing services (also called direct to bill) allow customers to make payments (such as utilities) or credit transfers via their mobile phone account balance without the use of a bank account, a credit card or a financial PSP. Once the user has signed up for the service, she/he is allowed to add money to the network account (using cash or by credit transfer). The user is then authorised to transfer money to other users through the mobile phone menu, using PIN-secured SMS text messages. Money can then be withdrawn from the mobile phone account, after it is confirmed that sufficient funds are available in the user’s account. Purchases made using direct mobile billing are charged directly to the user's mobile phone billing account.

In several developing countries this service allows users to send money to remote rural areas in a faster way. In Europe, for example, it is also widely used as a micro-payment method for gaming tokens, in-app items, or social network credits.

Mobile apps

Several mobile applications for payment services have been recently developed by financial institutions, telecommunications operators and merchants. Those apps allow customers to pay for goods and services directly from their smartphones or other mobile devices, or to make person-to-person payments. After installing the app, the users have to register and define the authentication credentials.

These apps can directly receive payment orders from merchants, requiring users to confirm the order via the app; or they can generate specific codes (including bar codes to be read by bar code scanners, as available, for example, in Austria) to be used by the customer to authorise the payment. With these services, card or account data are usually not transmitted at the POS.

In Bulgaria, for example, there is a payment systems operator that has developed a platform for mobile payments which allows cardholders to make payments and use other information services

through their mobile phones. Communication connectivity and data exchange are protected via the Public Key Infrastructure technology, which provides connection encryption and data integrity. The platform does not require card data to be stored in the mobile phone. The service uses a patented authentication technology, generating Payment Codes to be entered manually by the cardholder or the merchant instead of PIN.

Mobile apps also allow credit transfers, frequently between users of the same app, for which the receiver is chosen from the sender's contact list (by only associating the mobile phone number). These services are mentioned by several survey respondents, including Ireland and Portugal.

The charges can be made directly to the customer's bank account or card, if the app is associated with one of those; or can be included in the mobile network operator's monthly invoice.

Mobile wallets

Mobile wallets are a set of procedures agreed between a wallet provider and a consumer to use an NFC-enabled mobile phone as a proximity device to initiate payments using linked payment cards or accounts. As with online wallets, the user can associate a payment card or account, or upload money onto the account by using a card, a credit transfer or cash. Payments are allowed after the user's identity is confirmed (by entering a username and password), and the amounts are directly debited on the user's wallet account. The operations may be ordered through the app buttons or via a contactless solution. This service may be incorporated in banking tools made available to the consumers by their deposit and credit institutions, or offered by a third party.

Wallet services accessed by mobile devices can be used through mobile apps or SMS orders.[42] The most common procedure is the prior enrolment of the user by downloading an app.

Some specific entities have mobile wallets that allow their customers to make payments exclusively at their shops. These services are commonly used by restaurants / coffee-houses, public transport companies and car parking entities. Various coffee houses and parking companies provide their customers prepaid cards available through mobile apps, which allow payments by scanning QR codes or through the mobile apps.

In Canada, for example, there is a mobile wallet service that enables customers to make NFC-based payments whereby payment credentials are stored in the cloud, as opposed to the Secure Element broadly used by other services.

In Japan, for example, there are payment services called 'Osaifu-Keitai (mobile wallet)'. By downloading an app to a mobile device, such as a mobile phone or a smart phone, equipped with RFID IC chip, the mobile device can be used as a credit card or prepaid payment instrument (IC-card based type). Payment through the 'Osaifu-Keitai' uses wireless technology.

Recent studies show the increasing use and development of mobile wallets, in particular by merchants associations.[43] This market behaviour may be explained by a variety of different reasons.

[42] EBA, 2014; EP, 2015.

On the one hand, this phenomenon is driven by the Millennials, who are digital natives and avid purchasers who want to pay using simpler, faster and more user-friendly platforms.[44]

On the other hand, this market trend is not only associated with the merchants' aim of cutting costs (by reducing the bank fees applicable to the acceptance of payment instruments), but is also a result of the new emerging ecosystem of mobile payments.[45] Indeed, instead of focusing on "Know your customer", financial and non-financial payment providers, including retailers and MNOs, are accommodating their practice under the rule "know your customer's context".[46] As a result, merchants are using new mobile services - which are usually promoted as more secure, faster and simpler ways of payment, to reach new customers, offering them promotions and loyalty programmes. In addition, these innovative payment services give the merchants an insight into customer behaviour and profile ("customer context"), which they can use to leverage customer data to better advertise and sell their products.

Third party payment initiation

Third party payment initiation may also be a mobile payment service. In order to pay with this service, customers need to have previously installed the respective app (usually provided by a financial provider) on the mobile device.

In the Netherlands, the same provider of third party payment initiation in an online context also offers a similar service to be used in a mobile context. If the customer chooses to pay with this method, he must select the bank where she/he has her/his current account, after which the customer is asked whether she/he wishes to pay with the mobile banking app. In another step, the customer must log on to the app, follow the app instructions, and carefully check whether the amount and beneficiary details are correct. Afterwards, the payment automatically appears in the customer's bank statement. In addition, the bank also allows the customer to receive confirmation of the transaction with the payment details, through online banking or via email.

Barriers to the use of innovative payment services

The respondent jurisdictions reported various barriers to an increase in the use of online and mobile payments. Those barriers were referred to as being related to customers' security concerns and attitudes, the access to devices and infrastructures, the costs associated with payment services and the complex features of the technology in use.

---

[43] Chris Skinner considers that "card processing firms are fully aware that cards will be displaced by mobile wallets" (Skinner, 2014).
[44] Krishnan, 2014; Skinner, 2014.
[45] Krishnan, 2014. The author illustrates this emerging ecosystem of mobile payments, referring the example of an American retailers association that established a mobile payment network which allows its customers to pay by mobile phone application (using an associated mobile wallet) at participating retail stores, supermarkets, restaurants and gas stations.
[46] Skinner, 2014.

Security concerns and attitudes

The lack of confidence in payments security frameworks, due to security and privacy issues, was mentioned as a significant barrier to trusting in online and mobile payments. Customers express concerns that online and mobile payments are not secure and that fraud might easily happen.

Additionally, the lack of awareness of their availability and the manner how to use online and mobile payments are also referred to by the survey respondents as a barrier that hampers the growth of online and mobile payments users. Lack of knowledge on how to use these products leads to apprehension by consumers. PSPs have the responsibility to intensify information campaigns on the security procedures and advantages of using those services.

Also according to information assembled from the survey, digital payment services are still battling the cultural tendency to use traditional means of payment and channels, both in developing and developed countries. Baby boomers, or Generation X, are reluctant to move from traditional to innovative payment services still showing their preference for cash in daily payments.

Access to innovative services

The survey responses confirmed that innovative features of digital payment services require adequate supporting infrastructures, which are not equally developed between countries, leading to differences in the available payment services across countries. The underdevelopment of the infrastructures for online and mobile services, such as limited access to electronic devices, internet and/or mobile networks, or even electricity supply, are reported as significant barriers to the wider use of digital payment services.

Limitations also occur in access to services when the digital payment services are provided by entities other than banks that limit services to specific stores, private partnerships or specific customers' prerequisites or circumstances, introducing specificities to the use of the services and limiting the potential market for those services or instruments.

There are, as previously mentioned, various realities worldwide that contribute to a still unstable market of online and mobile payments, which strongly influences access by customers to innovative payment services.

Associated costs

Payment services and instruments have associated costs related to the effective use of the service, and costs related to the infrastructures and equipment needed to use such services.[47] Barriers associated with the costs of using online and mobile payment services and instruments were also referred to by the survey respondents.

The costs for users of innovative payment services and instruments can be higher when compared with the use of cash, due to the required registration for services, the need for adapted equipment, and additional fees and charges for the use of the services. In addition, there may also be hidden costs associated with the use of innovative digital payment services, of which the customer is not

[47] Hayashi, 2012.

always completely aware (for instance, in some cases, personal data are requested in return for using the services of the PSP).

In short, the initial cost related to innovative services may be high, driving consumers to withdraw from a wider use of digital payments.

The systems' features

The complexity of the systems used for online and mobile payments, when compared with traditional means of payments, act as a barrier to a wider development of digital payments.

Survey responses reported that the complex process of completing digital transactions, largely due to security measures, with various control levels, and identification processes, often related to 'Know Your Customer' forms required by PSPs and/or merchants, might discourage the development and adoption of innovative payment services, especially for small amount purchases.

PAYMENT PROVIDERS

Key points from the survey responses

- The number and diversity of PSPs are wide. Various providers are developing their activity not only on the online or mobile payments market, but on both.
- Deposit and credit institutions are now facing the competition of new PSPs in this market.
- In some countries non-financial providers are crucial to the digitalisation of payments. Non-financial providers have been gaining importance in the field of digital payments, contributing to innovative payment services.
- Jurisdictions' financial supervisory frameworks do not always cover all digital PSPs. Non-financial providers often fall out of the scope of supervisory authorities' mandate.

Overview

Providers of payment instruments and services available in online and mobile platforms have increased in number and diversity. Not only financial entities have been developing innovative payment services and instruments, but merchants and telecommunications networks are also developing innovative services to facilitate payments. On the one hand, financial institutions have the experience to provide payment services to their customers and are taking advantage of the new technology available to provide innovative payment services. On the other hand, merchants and telecommunications operators have access to the most recent technologies, have wide market penetration, and are extending their business to payment services.

Besides the clear differences in business models, the various providers also have different regulatory obligations and are subject to different levels of supervision. These differences need to be analysed from the consumer protection perspective.

Services developed by non-financial entities have led to a more competitive market that is especially tough for financial providers who used to be the sole providers of payment services. Financial entities are considered trustworthy to process payments, which is not always the case for non-financial providers.[48] This innovative market has forced financial providers to implement quick adjustments of their financial services, or to establish cooperation agreements with non-financial entities. According to the World Bank, although banks are still the main providers of innovative payment services, in several cases they are acting in collaboration with other entities. Non-financial providers have an important role in the development of innovative retail payment services, either on their own or in cooperation with banks.[49]

[48] Flatraaker, 2013.
[49] World Bank, 2012.

The responses to the survey show a significant variety of payment providers acting in the market, with various characteristics, and subject to different market conditions. There is not much information available on which providers have greater importance and market share, especially concerning those outside the financial supervisory framework. Thus, it is important to consider this matter as an international concern for debate.

Financial vs. non-financial providers

For the purpose of the report, the analysis of the providers of online and mobile payment services is divided into financial and non-financial providers, depending on whether their core activity is in the financial sector or not.

Financial providers

Payment services are widely available in the financial sector. Financial institutions provide various banking services related to bank accounts. Different payment services are available, including credit transfers, money remittances, transfer of funds to payment accounts, payment of bills, payments to the State, and direct debits, among others.

Financial institutions, in particular banks, were the first (and, for decades, the only) players on the payments market. They offered traditional financial products and services, such as payment cards, credit transfers and direct debits. Taking advantage of new technologies, the payment industry has developed rapidly and financial institutions now face competition from other providers.

According to Chris Skinner, "the bank of the future will connect intimately via mobile 24/7. It will not only be proactive, but predictive of customer needs and provide a connection not just to a payment or to money but to a financial lifestyle".[50]

However, digital payment services and instruments in general are similar to traditional ones, and are also associated with customers' bank accounts, but are available through online and mobile channels.

One of the first services developed by deposit and credit institutions was the home banking online service. This service was created to allow customers to access basic bank services from anywhere with an internet connection.

Besides deposit and credit institutions, other financial institutions also entered the retail payments market, having payment services as their core activity. These entities are not allowed to provide universal banking services or products, but only payment services and are usually designated as '**payment institutions'**. Payment institutions are often part of financial groups, acting as specialised entities in payments, or may also be part of commercial groups, acting as the financial firm specialising in payments.

There are also institutions dedicated to **electronic money services** (issuing and processing e-money operations). In some countries these entities are included in the 'payment institution' category, as is

[50] Skinner, 2014.

the case of Brazil. Other countries establish a separate category for those entities. In Armenia, for example, mobile operators willing to provide e-money services (such as mobile wallet services) have to establish subsidiaries specialised in issuing electronic money. Australia also considers these types of entities as providers of online and mobile payments, primarily as issuers of prepaid cards/account products, which may also be combined with digital wallet services.

In EU countries, the regulatory framework distinguishes between 'payment institutions' and 'electronic money institutions'. The framework establishes that all PSPs have to be registered and authorised by the national competent authorities, and have to adopt the specific requirements for 'payment institutions' or 'electronic money institutions'. According to the Payment Services Directive (PSD), 'payment institutions' are allowed to provide payment services, which include: (i) services enabling cash to be placed in a payment account; (ii) services enabling cash withdrawals from a payment account; (iii) execution of direct debits; (iv) execution of payment transactions through a payment card or a similar device; (v) execution of credit transfers; and (vi) money remittance. The Electronic Money Directive establishes that 'electronic money institutions' are allowed to issue electronic money, provide payment services and grant credit related to payment services, and provide operational services and closely related ancillary services in respect to the issuing of electronic money.

Financial institutions can also act as third party PSPs, when they make payments on behalf of their customers, initiating payment transactions. So-called account aggregators are third party PSPs. They are authorised by users to access their different online bank accounts, including credit cards and deposit accounts. This type of service could be seen as a means for financial institutions to expand their business in the online and mobile payments markets, competing with non-financial providers and offering new services to their customers. Poland reported the existence of online payment services delivered by payment integrators. According to EBA Guidelines on the security of internet payments, these integrators provide the payee (i.e. the merchant) with a standardised interface to payment initiation services provided by PSPs, being third party payment providers.[51] The funds are transferred to the merchant without entering the customer's credentials in the merchant's website.

Depending on the payment provider category adopted by the institution, different authorisations and capital and operational requirements are established, according to their different risk levels.

Non-financial providers

Non-financial payment providers may be understood as entities involved in the provision of retail payment services whose main business is not related to the financial sector. The developments in online and mobile payment services are strongly related to innovations developed by those entities acting in the non-financial sector. New players who are not traditional financial services providers are entering the payments market.[52]

The non-financial providers that have contributed the most to the development of digital payment services were internet operators, telecommunications operators and mobile network operators (MNOs), financial technology companies (Fintechs), merchants, and transport companies. These non-financial providers, in particular, are continuously exploring ways of interacting with their customers,

[51] EBA, 2014.
[52] EC, 2015a.

integrating their distribution channels for products, and providing services which are faster, more convenient, more responsive and more tailored,[53] representing a significant driving force in the development of payment services. They have a strong market position and have an improved ability to exploit market opportunities compared to traditional financial providers.[54] While traditional payment service providers, such as banks, are very reliant on their branches and define their commercial strategy based on the role of payment accounts as the traditional gateway to consumers, new entrants in the payments market have the potential to drive cross-border solutions and seize new markets from incumbents.[55] The increasing role of new providers, in particular, non-financial providers in the payments market is evident in all payment process stages and across all payment services.[56]

Online and mobile network operators have developed services associated with their communication services, benefiting from the wide market penetration already implemented. The payment services provided by those entities are, in some cases, related to the mobile account balance, and, in other cases, associated with payment cards or accounts held by the customer. In relation to merchants, payment services developments are usually related to the payment of goods and/or services at their online or physical shops (this service is broadly used, for example, by restaurants and coffee houses in Canada). As for transport companies, developments were mainly made by parking companies and public transport companies. Services may include, for example, online services to charge private accounts, which can then be accessed and used for payments through mobile services.

In developing countries, telecommunications network operators have performed a key role in the population access to new channels to make payments. This is especially true for mobile payments. A renowned case of a mobile money model developed by a telecommunications network operator is Kenya's m-payment model.[57] Its success contributed to the financial inclusion of a significant group of individuals. The Kenyan mobile money service was initially created to facilitate microfinance-loan repayments, and quickly developed into a wider money transfer scheme between network users, facilitating access to payment and transfer services without the need for a bank account.

Consumers International reported that in developing countries about one billion people did not have a bank account, but did own a mobile phone, and this number is expected to increase.[58] In developing markets, mobile channel is a major driver of financial inclusion.[59]

The increasing role of non-financial entities in the payment services market creates a number of concerns for regulatory and supervisory authorities.[60] Although authorities recognise the role of non-

[53] EC, 2015a.
[54] Flatraaker, 2013.
[55] EC, 2015a.
[56] The new Payment Services Directive (PSD2) embraces new business models of (non-financial) providers, where the PSP does not facilitate payments, but, for example, facilitates account information services, such as software which can be used by consumers to collect, organise and categorise all their personal transactions.
[57] FCAC, 2015.
[58] Consumers International, 2014.
[59] King, 2013; Krishnan, 2014.
[60] BIS, 2014.

financial PSPs in this market, there are also significant concerns regarding the safety and efficiency of the payments market.[61]

[61] The kind of business model of PSPs should also be considered by supervisors as a concern.

SECURITY RISKS

Key points from the survey responses

- The gradual sophistication of fraud schemes is identified in the survey responses as a relevant concern regarding security of digital payments.
- Deceptive practices and lack of reliability of devices and infrastructures are referred to as other causes of security incidents in online and mobile payments.
- Information regarding the main security incidents that occur in the use of online and mobile payment services are usually not available.
- Regulators and supervisors are developing initiatives to mitigate security risks in order to prevent fraud and increase consumer protection very often with non-financial competent authorities. International *fora* are issuing guidance on security standards. Payment industry associations are also adopting codes of conduct to increase security for online and mobile payments. Cyber security is at the top of the agenda.

Overview

Technological developments in online and mobile payment services have mainly sought to increase efficiency and security.[62] Reality, however, has shown that the pace of innovation in technological aspects is not always followed by an equivalent investment in security, leading to an increased potential risk of fraud. These potential weaknesses in security and reliability may affect the effectiveness and efficiency of innovative payment services to the detriment of users. These weaknesses may arise from the complexity of the technology and the processing around innovative services, and may also be a consequence of consumers' lack of precautions.

The FCA's 2014/15 Business Plan includes a section that presents its views on the main risks facing the financial sector in the UK. Innovations in online and web-based channels are identified as risks due to the fact that while digital advancements can make financial services faster and more convenient, foster competition in the market-place and reduce costs, they can also increase security and resilience risks that may arise from cyber-attacks or weaknesses in the underlying IT infrastructure.[63]

Security is perceived as one of the factors measured by customers when choosing payment services, in addition to costs, efficiency and convenience. Security in the processing of digital payments is mainly related to the correct identification of the payer and the secure transmission of identity and payment data.

[62] BIS, 2012.
[63] FCA, 2015.

In an attempt to **mitigate security risks** that arise from the use of online and mobile payments and to enhance consumer protection, competent authorities, international bodies and industry associations have been developing initiatives to mitigate security risks related to digital services, and to improve consumer trust in innovative payments. When implementing security standards, competent authorities face conflicting demands. Security requirements need to be strong to protect users. However, increasing security requirements should not jeopardise consumer convenience, and the efficiency of these innovative payments. Tougher security standards should not prevent innovation in the payments market either. Regulators and supervisors need to bear in mind that strong security standards may discourage the use of innovative payments and affect the development of those payments by the industry, calling for a risk-weighted approach.

Respondent jurisdictions mention security incidents as one of the main barriers to the growth of digital payments. Although they were not able to report data on security incidents, the main security types of incidents are identified as well as various risk mitigation initiatives. Some of those initiatives are more focused on promoting additional technical measures related to the payment systems, whereas others concentrate their work on awareness initiatives targeting users.

Main security incidents

Security risks are a significant concern for users of online and mobile payments. The risk of fraudulent access or unsecure transmission of personal or payment data are the main threats related to online and mobile payment services. Nevertheless, responses to the survey report that information about the frequency of incidents occurring in online and mobile payments is not widely available and only a few respondents indicate having some information through complaints analysis. Jurisdictions that report having some data from the complaints analysis do stress, however, that information is still quite scarce and has not captured a significant number of incidents on online and mobile payments.

Jurisdictions report not having any data that may be used to assess whether incidents are more frequent in online or mobile payment services. Although there is no statistical evidence, several jurisdictions report that online incidents may be more frequent, as the online payments market is more frequently used and is more developed within the country compared with the mobile payments market.

The lack of information is contributing to a less rigorous market understanding and analysis, which may impact on the effectiveness of the regulatory and supervisory response.[64]

As a tool to better monitor security incidents in the EU and to allow the adoption of accurate measures by competent authorities, the EBA Guidelines on the security of internet payments which entered into force on 1 August 2015, require PSPs to report major payments security incidents. Based on the survey responses and desk-based research, the following types of incidents were identified: fraud, deceptive practices and lack of reliability of devices and infrastructures.

[64] Furthermore, the lack of IT supervisors experience is also an important concern, when there are technological developments, digital channels and new players, sometimes with complex businesses models.

Fraud

The majority of respondents indicate **fraud** as one of the main and increasing types of security incidents occurring with online and mobile payment users.

The **theft of personal data and security credentials** is a common fraud in online and mobile payment services. Identity theft occurs when someone fraudulently obtains the user's identity to perform purchases in online or mobile platforms or other criminal acts, namely by compromising bank information.[65]

The incidence of this type of incident is high in CNP transactions, due to the difficulties that arise for merchants in verifying whether or not the purchase authorisation has been given by the real cardholder in an online transaction. CNP payments are, therefore, strongly exposed to identity theft attacks. In 2013, according to the ECB, CNP payments (i.e. payments via the internet, post or telephone) registered an increasing level of fraud, achieving a total of 66% of all fraud losses on cards issued inside the SEPA area. The report also suggests that CNP fraud has grown in the last two years at a higher rate than the respective transactions. In order to raise the security of internet payments, as of 1 August 2015, PSPs in the EU must implement a minimum set of security requirements.[66]

Canada's response also refers to identity theft mainly related to the CNP fraud, whose risks have been amplified due to the popularity of online payments. Canada considers that this type of fraud has been identified as a serious concern by electronic payment facilitators, since it is difficult for merchants to verify if the actual cardholder is indeed authorising the purchase on CNP payments. Brazil also mentions concerns with identity theft incidents, namely frauds with credit card (unrecognised purchases) and unrecognised banking transactions (e.g. credit order documents, available electronic transfers, banking billet payments). In China, the main concerns are also related to unauthorised transactions by hackers, privacy leaks and fund embezzlement. Japan also indicates concerns about fraudulent home banking transfers through which amounts are unlawfully transferred to other accounts and withdrawn unlawfully against the users will. France's response associates the risk of identity theft to lost or stolen cards or usurped numbers.

The risk of identity theft may also occur in fraudulent attacks based on **profiling and tracking techniques**. The techniques are based on the combination of aggregated databases with user personal data, enabling the identification of a person's habits, interests and other personal information. Profiling involves aggregating large amounts of user data and mining it to predict and shape user behaviour.[67] The possibility of identifying an individual increases when profiles are combined with location, tracking data and personal data stored on a mobile device, such as photos and contacts. Canada, for example, mentions profiling and tracking as a security incident occurring with mobile payment services.

Malware installations, **phishing attacks** and **SIM card swap attacks** are other types of fraud, performed by hackers to intentionally thieve personal data from online and mobile users.

[65] FBI, 2015.
[66] ECB, 2015.
[67] FCAC, 2013.

Malware, which is short for malicious software, is a general term for the type of software programmes that are designed to disrupt devices' normal functioning, gather personal information, or obtain access to private computer systems. The attacks with malware were referred to in the survey responses by Indonesia and the Netherlands. In Japan, fraudulent home banking transfers have increased in recent years. According to the report published by the National Police Agency, the number and amount of fraud transfers increased sharply in 2013. One of the reasons for the recent increase in fraud transfers is the use of more advanced and sophisticated methods such as malware that automatically processes illegal money transfers.

The most common **phishing** practice is sending "emails that appear to be from reputable sources with the goal of influencing or gaining personal information".[68] In order to lure the victim into giving sensitive information, the message might include a call to action such as "verify your account" or "update your personal information". Once passwords or other personal credentials have been revealed, phishers can use the victim's account for fraudulent purposes or to spam other online users.[69] Several jurisdictions refer to home banking phishing as an area that still requires attention.

A number of phishing variants have been developed to exploit different communication technologies, targeting victims through automated redirects to a bogus website (pharming), SMS (SMS phishing or smishing) or phone (phone phishing or vishing).[70]

Pharming is a fraudulent method that happens when a provider's URL is hijacked and the consumer is redirected to a fake site, or when fake apps are provided on mobile devices.

SMS phishing or smishing consists of sending a text message to an individual's mobile phone in an attempt to get her/him to provide relevant personal and financial data. A smishing attack usually contains a call to action to the intended victim, and requires an "immediate response".

Finally, phone phishing or vishing is the criminal practice of using the telephone system to gain access to personal and financial information from users for the purpose of committing fraud.[71] Some sophisticated attacks combine vishing and traditional phishing in which a phishing email is sent to an online user stating there has been a problem with an online account, which appears to be from a legitimate company such as a bank, credit card company, or online retailer. The email then directs the user to call a number and enter certain information to verify their account.[72]

SIM card swap is another kind of fraud related to online payments. SIM swap fraud occurs when a user's mobile phone is attacked and the incoming phone calls and SMS, including OTP, are fraudulently received by a SIM card in the possession of the fraudster. In South Africa, **SIM card swap** stands out among the increasing concerns.

[68] Hadnagy, 2015.
[69] EMC, 2009.
[70] Europol, 2015.
[71] EMC, 2009.
[72] EMC, 2009.

Deceptive practices

Commercial practices performed by online and mobile payment providers are not always clear and fair to the users of those services. As payments are often carried out without the presence of a physical operator, users are not always aware of the terms and conditions accepted by using those payment services, subscribing to that service, or buying that product on a digital platform.

Subscription traps are a type of deceptive practice, commonly referred as "too good to be true deals", in which the user discloses personal data (including payment card or account details), for a trial period service or to get a gift, but it turns out to be a subscription to various services with regular fees and costs. These traps usually encourage the user to enter deals that result in continuous payments.[73] Subscription traps are identified as an increasing type of security incident in online and mobile platforms, namely by Canada and Latvia.

Practices of '**cramming'**, which are direct-to-carrier billing frauds, consist of placing purchase charges directly on a bill (commonly a mobile phone bill), as occurs for example with the payment of downloaded digital content through a mobile phone. Cramming occurs when a third party adds small charges to a bill without the subscriber's permission. Canada and Latvia have identified this practice as an increasing fraud in their responses.

The Canadian response to the survey mentions that many people are unaware that a third party can be allowed to place charges to their mobile bill, and that 'cramming' can constitute a threat to the perception of direct-to-carrier billing as a trusted payment option. Attackers of this type of fraud count on consumers not reading their mobile bills, as the charges are often reported in a vague and deceptive manner.

The response from Latvia refers to problems with stopping automatic payment services (subscriptions) and problems with automatic applications of repeated payments. The Latvian response also refers to 'premium payments', which are the most common mobile payment method, as the most problematic type of mobile payment. Premium SMS or Premium calls are used as a mobile payment transaction initiation tool, and often are also used as a contracting tool (consent representation). The most problematic area in the scope of Latvian consumer protection is related to subscription services, where Premium SMS/calls are used for initial payments and afterwards repeated automatic billing via mobile invoicing or prepay debiting is applied.

Lack of reliability of devices and infrastructures

Online and mobile payments also carry specific risks related to the **reliability of devices**, **wireless connections** and **payment infrastructures**. Indeed, computers, laptops and mobile phones store personal information, which may lead to a major **data breach** in the case of loss or theft. Security weaknesses in wireless carrier infrastructures can put the users' data at risk. Some innovative services focus essentially on efficiency and do not have adequate and proper secure payment precautions.

Canada, for example, refers to the fact that payment services with NFC technology, such as NFC-based mobile wallets, can also incorporate specific risks for its users. The potential risk to consumers

[73] Cf. http://www.anpdm.com/article/4140594B78454B5A4575434B5B4171/14836586/2582840.

is related to the NFC antenna, which transmits a signal during a payment transaction. With this wireless data transmission, hackers can intercept the signal and collect information using a receiving NFC device. Due to this potential risk, NFC technology has been subject to a number of security features that protect consumer data.[74]

Some respondents report **malfunctioning of online and mobile payment infrastructures**. Bulgaria identifies incidents that occur when online payment services are occasionally unavailable, while Estonia and Indonesia report cases where payments are not executed due to technical shortcomings or system failures. The low capacity of infrastructures to support large amounts of data was also mentioned. Ireland's response refers to service outages that occur in financial institutions that have old IT systems; when new technology and upgrades are added, problems occur which may cause loss of access for making and receiving online payments. The UK is also worried about this, since the increasing use of online and mobile banking and payments means that firms' IT systems will increasingly come under pressure and may require additional system capacity to be able to deal with these volumes. There have been some recent outages of mobile services of large UK banks which have been the result of an inability to cater for large transaction volumes.

Causal drivers of security risk

The complexity around the functioning and processing of online and mobile payments seems to be a significant contributor to the occurrence of security incidents. The number of entities involved in providing an online or mobile payment service is generally wide (financial service providers, MNOs, retailers, and also social media in certain cases), and the rules applicable to each entity are usually different.

Online and mobile payment services tend to be based on complex IT systems that are not always understood by users, regulators, supervisors and merchants. When new technology is added and upgrades are made, some financial institutions with old IT systems face problems, namely service outages that can cause loss of access to make and receive online payments.

PSPs do not always control the whole supply chain of the payment processing, nor the technology and infrastructure security measures involved. Many aspects are under third party control and payment providers do not have an opportunity to mitigate the risk. For example, financial PSPs are usually responsible for the protection of customers' personal data, but they have no control over the devices used for the purchase.

The motivation for most data thefts is largely financial, and according to the Europol director in a Reuters' interview, a change has happened.[75]

"Banks, rather than their customers, are increasingly the main target of online thieves". In the interview, besides citing several cases of losses that have been reported in the media, the Europol director revealed that many more were never made public and that these losses show "a level of capability that is getting higher all the time, and perhaps runs the risk of outstripping the ability of the

[74] FCAC, 2013.
[75] Sterling, 2015.

banks to deal with it". He expressed that hacking attacks on banks were remarkable in terms of "the level of sophistication, in terms of the malware that's being used, and in terms of the sophisticated social engineering to identify the most important personnel among the banks' employees". He also mentioned that banks need to improve their defences, especially by understanding which employees were most vulnerable to attack and which in turn had authority over vital infrastructure. "It is raising serious questions about even the health of the financial services industry"

Rob Wainwright, 2015

Risk mitigation initiatives

The developments in online and mobile payment services were regularly followed by an increase in fraud concerns about online and mobile payments. Authorities and PSPs have therefore devoted special attention to the development of a secure and efficient payment environment. Various initiatives have been developed to mitigate security risks in online and mobile payments, and also to increase consumers' confidence in those new payment services.

National initiatives

Cooperation initiatives between national authorities can contribute to a more secure environment in online and mobile payments.[76]

The competent national supervisory authorities play an important role in the mitigation of security risks associated with online and mobile payments. Besides their normal competencies and tasks on the regulation and/or supervision of the market, it is also common for supervisory authorities to develop initiatives on their own or in cooperation with other national authorities. Initiatives may focus on providers, requiring the strengthening of their controls and the use of the highest standards for their security systems aiming to ensure high customer protection.

As non-banks are gaining size in the digital payment services market, non-financial competent authorities are also being involved in the regulation and supervision of the innovative payment services. Cooperation among authorities contributes to a more consistent and comprehensive common approach and is of crucial importance for different objectives, such as security, solvency of providers, efficiency, innovation, and financial inclusion.

Several examples of cooperation show the diversity of authorities that can contribute to a safer payment environment. In Spain, for example, the Central Bank collaborates with several national authorities, such as other financial supervision authorities, Parliament specific working groups, the National Ombudsman ('Defensor del Pueblo'), the Consumer Protection Regional Authorities, the anti-money laundering national service, Courts of Justice, and the Police. In Canada, the Financial Consumer Agency of Canada (FCAC) collaborates with provincial/territorial regulators, self-regulatory bodies and a number of federal oversight bodies, including the Office of the Superintendent of Financial Institutions, the Bank of Canada, the Canada Deposit Insurance Corporation, the Department of Finance, the Office of the Privacy Commissioner of Canada, the Financial Transactions and Reports Analysis Centre of Canada.

[76] BIS, 2012.

Japan's Financial Services Agency cooperates with relevant ministries, including the National Police Agency, and with financial industries to prevent fraud especially in transfers made through home banking services. The aim is to have financial institutions strengthening their security systems and giving warnings to customers. In addition, in 2015 the JFSA adopted a set of initiatives which aim to mitigate security risks:

- Requesting financial institutions to actively take measures to prevent fraudulent home banking transfers;
- Putting fraud transfers as one item of 'Focus of Monitoring' in 'Financial Monitoring Policy for 2014-2015';
- Revising several Supervisory Guidelines (such as 'Comprehensive Guidelines for Supervision of Major Banks'); and
- Starting to review whether financial institutions consider and introduce security measures in accordance with the level of advanced and sophisticated criminal methods, and whether financial institutions provide examples of security measures that customers are required to take and call their attention.

The Indonesia FSA reported it was working closely with the Bank Indonesia, as the regulator in payment system, ensuring payment system supervision and regulation are in place. These authorities also work closely in monitoring incidents, considering that many of those incidents can be resolved by improving risk management and technology within a bank. Recently, the Central Bank required the implementation of additional security measures for debit and credit cards, such as the introduction of a 6-digits PIN, as well as the adoption of actions to decrease security risks. The Bank Indonesia has also required all merchants to use PIN instead of card holder's signature to execute both debit and credit card transactions. Additionally, the Indonesia FSA has been requiring banks to increase technological and system reliability, conducting on-site supervision to assess the conditions and to improve their complaint handling process, to ensure all complaints are handled professionally, fast and fair, and the bank has necessary actions to mitigate the risks. The Indonesia FSA has also strengthened its coordination with the banks, encouraging them to share any information related to any indication or alert of fraudulent online or mobile payment.

In Ireland, the Competition and Consumer Protection Commission, which is the national entity responsible for the enforcement of competition and consumer protection law, promotes consumer awareness of scams by informing consumers of the various types of scams in its newsletters and website. Furthermore, the Central Bank is obliged to make a report to the Garda Síochána, the national police force, if the Central Bank becomes aware of, or suspects that a supervised institution has committed a criminal offence or an infringement of the Criminal Justice Act (Money Laundering and Terrorist Financing) 2010.

In Saudi Arabia, the Banks Media Committee launched various campaigns relating to information security and awareness. On the other hand, the 'Information Security Committee', involving the Saudi Arabian Monetary Agency and domestic banks, meets each month to share incidents, risks and good practice. This creates awareness and helps banks take preventive action.

Brazilian regulation imposes responsibility on the PSP with respect to the security of the products and channels it provides. Historically, that provision has given good incentives to the PSP to properly manage its risks and has resulted in relatively few frauds. Online PSPs have kept up with changes in cyber-attacks and promptly reacted by developing security services.

Payment system oversight in Austria has a so-called "risk-based approach" that prioritises the assessment of payment systems that suffer from an increase in incidents or have a higher risk exposure due to the introduction of new technology, for example.

In the Netherlands, measures to mitigate security incidents were effective. Malware attacks against home banking have been significantly reduced through the use of automated transaction monitoring. Skimming fraud (debit cards) also fell significantly, mainly by geoblocking which blocks the cards outside the EU.

The survey response from Luxembourg reported that the licensed entities must have in place a risk policy, covering the specific risks inherent to the business (such as fraud, misappropriation of funds, IT incidents, break downs, etc.).

Philippines also reported several initiatives to mitigate security risks regarding online and mobile payments, among which the implementation of confirmation and identity checks to significant transactions or activities, the strengthening of infrastructure and security monitoring, the adoption of appropriate authentication techniques, the issuance of public warnings and the issuance of regulations on several related matters, such as consumer protection, outsourcing, anti-money laundering, e-money operations, remittances and information technology risk management. Furthermore, the Central Bank has recently approved the creation of a new unit, within the Core Information Technology Specialist Group, dedicated to thoroughly study cyber-security threats with the aim of continuously enhancing the regulatory framework and institutionalising cyber-security due diligence within the financial industry.

International cooperation

Countries and international bodies have established cooperation initiatives to deal with security, which is a common concern.

The focus on security risks in online and mobile payments has gained a worldwide scale, not only because it is an issue in almost every developed and developing country, but also because a single payment process may involve more than one jurisdiction. Cross-border payments or payment operations processed by global entities increase the need to develop worldwide cooperation arrangements for a more cooperative oversight and a more standardised supervisory approach.[77]

The OECD, through the G20/OECD Task Force on Financial Consumer Protection, developed a set of high-level principles in 2011 on consumer protection in the field of financial services to respond to the call from the G20 Finance Ministers and Central Bank Governors, the FSB and other relevant international organisations. In 2014, the Task Force published its Action Plan that defines the effective approaches to support the implementation of the high-level principles on financial consumer protection, which includes approaches regarding the regulation and supervision of new products, technologies or delivery channels.

The OECD is also working on online and mobile payments through the Committee on Consumer Policy, which is an intergovernmental forum addressing a broad range of consumer issues. In 2014,

[77] BIS, 2012.

the Committee issued new policy guidance to enhance consumer protection in mobile and online payments.

The ECB, as the central bank for Europe's single currency, has, among other functions, the statutory task of promoting the smooth operation of payment and settlement systems in the euro area, which comprises 19 EU countries. In 2011, the ECB set up the SecuRe Pay, a cooperation initiative between supervisors of PSPs and overseers. SecuRe Pay promotes common knowledge and understanding regarding the security of electronic retail payment services and instruments provided within the EU. Currently, the SecuRe Pay is co-chaired by the ECB and the EBA. In 2014, the EBA, as a regulatory authority, published *Guidelines on the security of internet payments*, which are based on the SecuRe Pay Recommendations.[78] These Guidelines strengthen the legal basis for the implementation of harmonised oversight and supervisory policies on retail payments across the EU. For example, issuing PSPs will have to support strong customer authentication for the initiation of payments and access to sensitive payment data, while the PSPs offering acquiring services will have to support the issuer PSP for this purpose.[79]

The EBA has also included in its activities a Standing Committee on Consumer Protection and Financial Innovation and a Task Force on Payment Services. EBA aims to monitor new and existing financial activities, promoting the safety and soundness of markets and convergence of regulatory practice.

Self-regulatory initiatives[80]

PSPs have also adopted a set of self-regulatory initiatives to minimise potential frauds and the impact of effective fraud on customers and on themselves.

National regulatory and supervisory authorities are not the only entities concerned with the security-related issues of online and mobile payments. PSPs are also worried about maintaining high security levels to safeguard their reputational risk.

The adoption of combined and dynamic security credentials enhances the security of digital payment services. Besides passwords, code cards and PINs, new and innovative forms of authentication have been introduced by providers, such as OTPs sent by SMS, tokens, or even biometric readers. Additionally, the password protection of electronic devices (e.g. laptops, tablets, mobile phones) introduces a second security layer. To benefit from all these security measures and protect the sensitive data that may be stored on devices, it is of the utmost importance to protect devices from malicious software and hacking attacks.

In various countries, the financial industry has developed security measures and guidelines to contribute to risk mitigation. In Canada, the Canadian Code of Practice for Consumer Debit Card Services has been extended to online transactions through the Canadian Bankers Association's customer commitment concerning online payments. Under this public commitment, Association members undertake to apply the principles and provisions of the Debit Card Code to online payments associated with customer deposit accounts. Another related commitment is the Interac Online

[78] ECB, 2013a; EBA, 2014.
[79] ECB, 2015.
[80] Self-regulatory initiatives are also described in the chapter 'Regulatory framework'.

Customer Commitment. The regulated financial institutions offering online debit payment services via Interac Online have committed to providing customers with appropriate disclosures related to: any fees associated with Interac Online services; the customer's responsibilities for protecting passwords and the consequences if these are violated; whom the customer should contact in the event of a problem; and the potential extent of losses resulting from unauthorised use of Interac Online services. Furthermore, merchants who offer Interac Online are required to comply with the Canadian Code of Practice for Consumer Protection in Electronic Commerce. The Code establishes merchant benchmarks for good business practices related to disclosure of information, contract formation and fulfilment, online privacy, security of payment and personal information, redress, unsolicited emails, and communications with children.

The Canadian financial industry, with the participation of banks and credit unions, has also developed guidelines on mobile payments. The Canadian NFC Mobile Payments Reference Model provides a level of security to mobile payments that employ NFC technology. It describes guidelines related to the design of m-payment applications, the installation of these applications on mobile devices, the collection and storage of data, and the execution of mobile payments themselves.

In Japan, the financial industry has worked on strengthening security measures and warning customers. Some financial institutions have successfully reduced fraudulent home banking transfers and their consequences by combining the following measures: they do not accept immediate transfer when the beneficiary is designated at each transfer, they do not accept increases (changes) to the amount of transfer limit via online, and they monitor whether there is anything peculiar with a payment instruction transaction.

There are also initiatives developed by non-financial associations. This is the case of Austria, for example, where a private initiative ("Austria Wallet") was developed by Austrian companies of various industries (payment, banking, technology, telecommunications, etc.) aiming at developing a common national technical standard for mobile payments.

International bodies, from the finance sector and the network and security sector, have also developed self-regulatory guidance on security concerns. These initiatives not only increase the adequacy of security measures, as they are developed to establish effective security controls and measures, but also give supervisory authorities guidance on the security measures adopted by the supervised entities.

A group of international PSPs has also developed a set of robust and comprehensive standards and supporting materials aiming to improve the security measures adopted in payment card services. The *Payment Card Industry Data Security Standards* (PCI DSS Standards) include a framework of specifications, tools, measurements and support resources that assist any business that stores, processes or transmits payment cardholder data, for safe handling of cardholder information during the payment operation processing.[81] These Standards contribute to a better coordinated payments security environment, especially important in cross-border operations.

There is also the 3D-Secure protocol, which is a solution that provides an additional level of security to online payments with debit and credit cards. This solution introduces an online authorisation

[81] ENISA, 2014; PCI SSC, 2015.

requirement to complete the payment process. The payer is redirected to her/his bank's website, where a password is required, typically an OTP which is sent as an SMS to the user's mobile phone.[82]

The International Organisation for Standardization (ISO) has also published standards on information security management systems (ISO/IEC 27001:2013), business continuity management systems (ISO 22301:2012), and universal financial industry message scheme (ISO 20022). ISO 27001 stipulates requirements for improving information security management systems in an organisation and for the assessment and treatment of information security risks. ISO 22301 specifies requirements to improve a documented management system to protect against disruptive incidents. ISO 20022 sets out a standard for electronic data interchange between financial institutions, establishing a single, common "language" for all financial communications.[83] Large international banking groups adopt internal practices based on the ISO standards, guaranteeing the ISO certification of their IT governance strategies.[84]

PSPs of new payment services, in particular technological and software developers, are permanently monitoring the market in order to develop more secure and inviolable ways of authentication. An example of the industry contribution is the development of biometric procedure authentication, by using the fingerprint, the iris or the heartbeat as verification.[85]

Regarding the protection of users of online and mobile platforms, there are two important international *fora* – the Anti-Phishing Working Group and the Anti-Phishing Mobile Working Group – where different stakeholders, such as financial institutions, retailers and solutions providers, can meet, specifically focusing on unifying the global response to cybercrime. These Groups provide a forum for counter-cybercrime managers to discuss phishing and cybercrime issues, consider potential technology solutions, access data logistics resources for cyber security applications and cybercrime forensics, cultivate the university research community dedicated to cybercrime and advise government, industry, law enforcement and treaty organisations on the nature of cybercrime.[86]

Financial education initiatives[87]

Education is a key priority for the mitigation of risks caused by customers' lack of awareness.

Well informed customers of online and mobile payment services will have a more cautious use of those services. Education should not only cover financial topics, but also the technological features associated with mobile or online payments.

Luxembourg and Spain reported in the survey, as a causal driver for incidents, the insufficient or unclear information for consumers.

---

[82] It should be noted that the payments industry is adopting this solution to comply with strong customer authentication requirements in several European jurisdictions.
[83] Cf. http://www.iso.org.
[84] ENISA, 2014.
[85] Skinner, 2014.
[86] Cf. http://www.apwg.org/.
[87] Financial education initiatives are detailed in the chapter 'Supervisory framework'.

Financial education initiatives have been developed by several jurisdictions. In some cases, they are part of the regulatory or supervisory authorities, and in other cases the financial sector organisations play an important role, considering their wide geographic coverage and their proximity to the users.

The OECD, through the International Network on Financial Education (INFE), has also set up a work stream to study the implications of digital financial services for financial education and related financial consumer protection issues.

REGULATORY FRAMEWORK

Key points from the survey responses

- There are different regulatory frameworks adopted by the respondent jurisdictions, as regards the services and providers covered.
- Several jurisdictions have a regulatory framework that covers payment instruments and services regardless of the channel, as is the case of EU Member States. Other jurisdictions, such as Saudi Arabia and Canada, developed regulatory acts specifically focused on digital payment services.
- Various jurisdictions are following the guidance issued by international bodies, regarding security issues in online and mobile payment services.
- Self-regulatory initiatives developed by providers and industry organisations, both at a national and international level, are mentioned as playing an important role in addressing security risks.

Overview

The most important topic of regulation regarding innovative payments is security. According to the survey, national competent authorities are concerned about online and mobile payments' security requirements, stressing the importance of users' protection. Additionally, jurisdiction respondents reported that they are following guidance issued by international bodies in the security field. PSPs need to ensure the provision of payment services in a secure environment.

However, the regulation of online and mobile payment services and PSPs is still maturing worldwide. In some jurisdictions the existing regulation encompasses traditional and digital services without, in some cases, acknowledging the special features of these new payments. In others there are specific regulations for the innovative payments market.

Innovative payments are very often cross-border. Regulators should be mindful that the majority of new digital services are provided across countries, which in turn requires a transnational action plan and close cooperation with other regulators and agencies. In the EU, for example, the European authorities have been addressing these new challenges by issuing regulations, standards, guidelines and opinions aiming to increase security of these new payment services.

Although security issues are now and will most probably remain at the top of the national and international agenda, regulators are also challenged to address other crucial consumer protection topics, being disclosure of information one of them.

National framework

In EU countries, retail payment services are regulated by a comprehensive and compulsory framework, establishing common standards within Member States. With the aim of creating an EU-wide single market for payments, the regulatory framework contributes to the efficiency of cross-

border payments within EU countries. The scope of the regulatory framework does not take into consideration the way or the platform used to provide the payment service, and therefore, online and mobile payments provided within the Community are also covered by this payment services framework.

The main initiative regulating payment services and their providers in the EU is the Payment Services Directive (PSD).[88] The PSD lays down rules concerning PSPs and transparency of conditions and information requirements for payment services (e.g. payment cards, credit transfers, direct debits, etc.) provided within the EU (the so-called "two-leg transactions")[89] in EU currencies, and the respective rights and obligations of payment service users and PSPs.

With respect to PSPs, the PSD establishes, on one hand, that only the six categories of PSPs specified in the Directive – (i) credit institutions; (ii) electronic money institutions; (iii) post office giro institutions which are entitled under national law to provide payment services; (iv) payment institutions; (v) the ECB and national central banks when not acting in their capacity as monetary authority or other public authorities; and (vi) Member States or their regional or local authorities when not acting in their capacity as public authorities) – can provide payment services and, on the other hand, that all institutions providing payment services within the EU have to be authorised by the national competent authority to carry out their payment activities throughout the EU.

Concerning transparency of information, the PSD establishes information requirements for PSPs. Providers shall make available to users clear information regarding the services they are providing. Prior to the payment service, information related to fees, complaint procedures and all charges payable shall be given by providers in an easily understandable way. Furthermore, after the execution of the payment transaction, providers shall disclose information to the payer regarding, namely, the reference of the payment transaction and of the payee; the payment amount; and the fees and other charges related to the transaction. Finally, the PSD establishes that any changes in the framework contract shall be proposed by the PSP no later than two months before their proposed date of application.

The PSD also defines rules on the responsibility related to fraud costs. It establishes that the PSP, where applicable, should give users a description of steps that they are to take in order to keep safe a payment instrument and how to notify the PSP in case of loss, theft or misappropriation of the payment instrument or of its unauthorised use. The PSP assumes the responsibility in case of unauthorised payment transactions, resulting from the use of a lost or stolen payment instrument or, if the payer has failed to keep the personalised security features safe, from the misappropriation of a payment instrument, unless it is proved that fraud was caused by customers acting fraudulently or with intent or gross negligence.

The PSD also lays down rules on charges, establishing that the PSP shall not charge the payment service user for the provision of information, and establishes several obligations to the PSPs and to the users in relation to payment instruments. For instance, PSPs should make sure that the personalised features of the payment instrument are not accessible to parties other than the user

[88] Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007.
[89] "Two-leg transactions", because the Directive only covers payments where both the payer and the recipient payment service provider are located in the EU. Cf. http://europa.eu/rapid/press-release_MEMO-07-152_en.htm?locale=en.

entitled to use the payment instrument and ensure that appropriate means are available at all times to enable the user to make a notification of loss, theft or misappropriation of the payment instrument or of its unauthorised use.

In 2013, a revision of this Directive was proposed by the EC, and the new Directive (PSD2) was published. This new Directive addresses new payment services and aims to ensure "protection of users and the development of a sound environment for e-commerce" by increasing security measures. It also acknowledges that "a solid growth of internet payments and mobile payments should be accompanied by a generalised enhancement of security measures".[90]

Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (hereinafter "PSD2") repeals Directive 2007/64/EC (PSD) and entered into force in mid-January. Member States must adopt and publish measures to comply with PSD2 by 13 January 2018.

The new Directive aims to promote the continued development of payments market, enabling new means of payment to reach a broader market, ensure a high level of consumer protection in the use of those innovative payments across the EU and make payments safer and more efficient.[91]

The PSD2's rules will have an impact on the online and mobile payment services market, namely by revising its scope, including new payment services, enhancing consumer protection in case of unauthorised transactions, and improving security measures. The definition of payment services embraced by the Directive remains technologically neutral and allows for the development of new types of payment services.[92]

Regarding the Directive's scope, some of its provisions on transparency and information requirements for PSPs and on rights and obligations in relation to the provision and use of payment services are applicable to payment transactions in all currencies where only one of the PSPs is located within the Union, in respect to those parts of the payments transaction which are carried out in the Union.[93] Additionally, the Directive clarifies the wording of some of its exclusions (e.g. the exclusion related to the use of payment instruments that can be used only in a limited way) and narrows the scope of other exclusions (e.g. the exclusion related to payment transactions by a provider of electronic communications networks or services provided in addition to electronic communications services for a subscriber to the network or service).[94]

With the emergence of new types of payment services, especially in the area of online payments, and given that technological developments have engendered a range of complementary services,[95] PSD2 embraces new and different payment services: the payment initiation service and the account information service. According to the legal wording, the first service is defined as a service to initiate a payment order at the request of the payment service user with respect to a payment account held at another PSP, while the account information service is an online service to provide consolidated

[90] Recital 95.
[91] Recital 6.
[92] Recital 21.
[93] Article 2.
[94] Article 3.
[95] Recitals 27 and 28.

information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.[96]

PSD2 reduces the limit on losses borne by the user relating to an unauthorised payment transaction, establishing a maximum of 50 euros if that transaction results from the use of a lost or stolen payment instrument or from the misappropriation of a payment instrument and there is no evidence that the user has acted fraudulently or failed to fulfil her/his obligations with intent or gross negligence.[97]

Taking into consideration that the "security of electronic payments is fundamental for ensuring the protection of users and the development of a sound environment for e-commerce" and that "a solid growth" of digital payments should be accompanied by a generalised enhancement of security measures,[98] PSD2 establishes that PSPs apply strong customer authentication where the payer accesses its payment account online, initiates an electronic payment transaction and carries out any action through a remote channel which may involve a risk of payment fraud or other abuses. This method of authentication is designed to guarantee safety, preventing the risk of fraud.[99]

Further, the Directive states that, in the case of a major operational or security incident, PSPs shall, without undue delay, notify the competent authority in the home Member State of the PSP. Considering the aim of protecting consumers from losses, PSD2 establishes that where the incident has or may have an impact on the financial interests of its payment service users, the PSP shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects on the incident[100]. Finally, the PSD2 states that "Member States shall ensure that PSPs provide, at least on an annual basis, statistical data on fraud relating to different means of payment to their competent authorities. Those competent authorities shall provide EBA and the ECB with such data in aggregated form".

The EU countries have also to apply the regulatory framework established by the Electronic Money Directive.[101] This Directive embraces electronic money institutions that can issue electronic money and provide payment services. Therefore, the providers of a significant part of the new prepaid electronic payment products, such as prepaid payment cards or electronic wallets, are covered by this framework.

In addition to the legal framework described, there is an important European initiative – the SEPA[102], which aims to promote the use of electronic payments (including payment cards, credit transfers and direct debits), by harmonising the requirements and the conditions of the transactions, rights and obligations of users and providers and the applicable charges.

Pursuing the aim of building an integrated and harmonised market for electronic payments, the EU legislator issued a Regulation that eliminates the differences in charges for cross-border and national

[96] Article (15) and (16).
[97] Article 74.
[98] Recital 95.
[99] Article 97.
[100] Article 96.
[101] Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009.
[102] The Single Euro Payments Area.

payments in euro.[103] It is applicable to payments in euro, but non-euro area Member States have the possibility to extend the application of this Regulation across the EU. The basic principle is that the charges for payment transactions offered by a PSP must be the same whether the payment is national or cross border.

Another step in SEPA implementation was made by a Regulation which provides the rules for the functioning of credit transfers and direct debits in euro in the internal market, excluding card-based payment transactions from its scope.[104]

In June 2015, the EU published a Regulation on interchange fees for card-based payment transactions. This Regulation intends to "help to develop an EU-wide market for payments, which will enable consumers, retailers and other undertakings to enjoy the full benefits of the EU internal market including e-commerce".[105] Considering that "card-based payment transactions" means, under the Regulation, "a service based on a payment card scheme's infrastructure and business rules to make a payment transaction by means of any card, telecommunications, digital or IT device or software if this results in a debit or a credit card transaction",[106] it implies that, by reducing the level of interchange fees, the EU intends to develop the electronic payments market, including online and mobile payments.

The EBA, as an independent EU Supervisory Authority, plays an important role in promoting the convergence of supervisory practices, working in the assessment of risks and vulnerabilities in the EU banking sector and promoting a transparent, simple and fair internal market for consumer financial products and services.[107] One of EBA's working areas is precisely "consumer protection and financial innovation".[108]

The EBA, being concerned about the increase in frauds related to internet payments, decided that the implementation of a more secure framework for internet payments across the EU was necessary. In this context, and before the revision of the PSD, in order to create a more secure, competitive and consumer-friendly set of rules for payments in the EU, the EBA issued the 'Guidelines on the Security of Internet Payments' in December 2014. The Guidelines were based on the Recommendations that had been developed and published by the SecuRe Pay in January 2013.[109] The Guidelines complement the requirements at both the EU and domestic level, requiring regulated financial service providers to have appropriate systems and controls.

[103] Regulation (EC) No 924/2009 of the European Parliament and of the Council of 16 September 2009.
[104] Regulation (EU) No 260/2012 of the European Parliament and of the Council of 14 March 2012.
[105] Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015.
[106] Cf. Article 2 (7).
[107] Cf. https://www.eba.europa.eu.
[108] Cf. Article
9 (2) of Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010.
[109] Secure Pay was set up in 2011 by the ECB as a voluntary cooperative initiative between authorities and is currently co-shared by the ECB and EBA. It aims at facilitating common knowledge and understanding, in particular between supervisors of PSPs and oversees, on issues related to the security of electronic retail payment services.

The EBA Guidelines, which entered into force on 1 August 2015, set the minimum security requirements for PSPs across the EU, and intend to provide enhanced protection of EU users against payment fraud on the internet. In particular, the Guidelines focus on *general control and security environment* (governance, risk assessment, incident monitoring and reporting, risk control and mitigation, and traceability), on *specific control and security measures for internet payments* (initial customer identification, information, strong customer authentication, enrolment for, and provision of, authentication tools and/or software delivered to the customer, log-in attempts, session time out, validity of authentication, transaction monitoring, and protection of sensitive payment data), and on *customer awareness, education, and communication* (customer education and communication, notifications, setting of limits, and customer access to information on the status of payment initiation and execution).

In accordance with the EBA Regulation, national competent authorities and financial institutions should make every effort to comply with the Guidelines ("comply or explain" principle). Twenty three national authorities in the EU stated that they will comply with the Guidelines, while two indicated partial compliance and three reported that they will not comply. In addition, two of the three EEA/EFTA authorities reported compliance.

In addition to the EU regulatory framework for consumer protection, some EU Member States adopt at national level specific consumer protection codes to regulate the conduct of providers when dealing with consumers. One example is the Consumer Protection Code introduced by the Central Bank of Ireland in 2006 (that was last updated in 2012), which sets out the requirements regulated providers must comply with when dealing with consumers in order to ensure a similar level of protection for all consumers, regardless of the type of financial service provider. In other countries, such as Bulgaria, Lithuania, Portugal and Spain, the national central bank is also competent to issue regulations – guidelines, policy statements, notices, circular letters, etc. – implementing legal acts or clarifying practices which should be observed by PSPs.

In a nutshell, EU jurisdictions follow a harmonised framework which in some countries is complemented with secondary regulations applicable to PSPs.

Outside the EU, some countries, such as Brazil, structure their regulations mainly using the EU Directives and Regulations as reference, whilst also taking their specific realities and idiosyncrasies into account.

The Brazilian regulatory framework embraces the conduct of business and prudential matters. The provision of payment services is regulated by law, which also empowers the Central Bank of Brazil (BCB) to discipline, grant licenses and oversee payment schemes and payment institutions' operations, in accordance with guidelines issued by the National Monetary Council (NMC).

The NMC, by means of the regulatory instrument known as "Resolution", laid down the guidelines that must be observed by the BCB when regulating payment schemes and payment institutions. The rules issued by the NMC to promote responsible, adequate and fair conduct of business of financial service providers, by establishing transparency, disclosure and suitability procedures, disciplining the fees charged to consumers and requiring the implementation of ombudsman components responsible for recording consumers' complaints and for acting as conflict mediator, also apply to payment service provision. In addition, payment institutions are required to implement internal control systems in order to comply with those regulatory requirements.

Payment institutions must also abide by the rules set forth in the Consumer Protection Code, considered the main instrument to protect consumers from inadequate business practices. This Code was complemented by several decrees, such as a decree obliging PSPs to grant easy and free-of-charge access to their customer service channel, which is used to provide information related to rendered services, register complaints and execute cancellation requests.

Furthermore, the BCB regulation is mainly executed through an instrument named “Circular”. On 4 November 2013, the BCB enacted a wide set of rules regulating payment schemes and payment institutions on the following topics: payment accounts, including prepaid and post-paid accounts; risk management procedures, corporate governance and minimum capital requirements required from payment institutions; types and coverage of payment schemes; requirements and procedures that a firm should follow in order to obtain a license to operate as payment institution and to appoint its board of directors. In addition, payment institutions shall adopt measures to prevent money laundering and terrorist financing.

In the past few years, the BCB has also disclosed periodic reports about the Brazilian retail payment industry, which was used as a focal point for recommending non-binding standards in order to improve the efficiency of the financial system.

Other jurisdictions have also issued regulations comprising both traditional and digital payments. In Japan, the Financial Services Agency, which is the entity responsible for the regulatory framework, has developed the ‘Banking Act’ and the ‘Payment Services Act’ which regulates not only fund transfer services but also payment services that are provided via prepaid payment instruments, including online and mobile payments. Each Act aims to keep the prudential nature of the financial system and the payment system and ensuring the appropriateness of conduct of business. Prepaid payment instruments are regulated by the Payment Services Act. This Act requires issuers of prepaid payment instruments to notify or be registered with competent authorities, maintain a security deposit equivalent to more than half the amount of payment instruments unused after issuance, and provide a refund in case of end of service.

In Saudi Arabia, the Saudi Arabian Monetary Agency (SAMA) has imposed a set of procedures on online payments, intended to avoid incidents of personal data misuse or theft. The Agency has required the use of a second factor for all online payments. Typically this will take the form of an OTP sent by the payment issuer (the payer’s bank) to the designated mobile phone of the account holder. SAMA has also stipulated that the account holder’s bank must send an SMS alert to the account-holder for every credit or debit posted to the respective account.

SAMA also developed regulations on Mobile App security and published the *Saudi Arabian E-Banking Rules*, issued in April 2010, to regulate home banking payments. This regulation is of a prudential nature with a legal underpinning. These *E-Banking Rules* specifically identify the nature and scope of the ‘risk’ manifest in ‘information only’ and ‘transaction capable’ internet services. They also identify the 14 Risk Management Principles that define the minimum requirements against which regulated entities (banks) offering e-banking services will be assessed (regarding Board and Management Oversight, Security Controls, and Legal and Reputational Risk Management).

Furthermore, SAMA issued the specific *Regulatory Rules for Prepaid Payment Services in the Kingdom of Saudi Arabia*, which regulates the issuing, acquisition and usage of prepaid payment services. Although these regulatory rules focus primarily on "cards", they are applied to all prepaid services, including smart/EMV cards and magnetic stripe card environments, as well as other form factors for prepaid payment services such as contactless and mobile payments.

As the legislative body responsible for exercising regulatory and supervisory control over banks and money exchangers, issuing general rules, ensuring all banks and money exchangers comply with and effectively implement the relevant laws and regulations, SAMA issues regulations on Multi-Factor Authentication, SMS Notification and Mobile App security.

In Canada, the consumer protection regulation framework applicable to online and mobile payments depends on the underlying source of funds and the type of the PSP. When a mobile payment service (such as a mobile wallet) or a payment source (such as a debit or credit card) is issued by a bank (i.e. a federally regulated financial institution), obligations associated with the Bank Act must apply. Furthermore, banks should observe a number of consumer-focused voluntary codes of conduct and public commitments. Non-bank providers may be subject to generic federal and provincial consumer protection legislation, may endorse voluntary industry codes of conduct, and may adhere to corporate policies that protect consumers in one way or another.

In addition, each province and territory has consumer protection legislation. Nevertheless, there may be similarities between jurisdictions on matters relating to consumer protection. For example most provinces have enacted internet agreement (or remote agreement) legislation for the purpose of protecting consumers online.

Concerning the use of NFC, the Canadian NFC Mobile Payments Reference Model provides a level of security to payment services that employ NFC technology. This is an initiative of the Canadian financial industry and describes guidelines related to the design of m-payment applications, the installation of these applications on mobile devices, the collection and storage of data, and the execution of mobile payments themselves. However, compliance with the Reference Model is voluntary and is not enforced by any oversight agency.

In December 2013, the Canadian Radio-television and Telecommunications Commission (CRTC) published a Wireless Code that is intended to better inform wireless consumers on the rights and obligations contained in their contracts. The Wireless Code applies to all “wireless services” (i.e. MNOs) but does not apply to other entities offering direct-to-carrier billing services.

The Wireless Code addresses a number of items that are relevant to direct-to-carrier billing. For example, contracts must state the rates for optional services that are selected by the customer at the time of the contract, and must indicate where customers can find information about rates for optional and pay-per-use services. The Wireless Code also states that a “service provider must not charge for any device or service that a customer has not expressly purchased.” Also relevant to the risks associated with fraudulent direct-to-carrier billing, the Code requires the service provider to inform the customer on how to unsubscribe from premium services.

Regarding personal data protection, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to organisations that collect, use or disclose individuals’ personal information in the course of commercial activity. It does not apply to organisations in provinces deemed to have substantially similar private-sector privacy legislation. PIPEDA continues to apply in cases of cross-border data flows. It also applies to federal works, undertakings, or businesses across Canada – including telecommunications companies as well as banks listed in schedules I and II of the *Bank Act* – where it covers both customer and employee personal information.

International guidance

In addition to the national regulatory framework and the EU initiatives, which are directly applicable to each jurisdiction within the EU, there is a set of international guidance regarding consumer protection regulation in the online and mobile payments market.

The OECD plays an important role in this field, recommending a set of policy guidance intended to help shape consumer protection and industry practices.

In 2000 the OECD published *Guidelines for Consumer Protection in the Context of Electronic Commerce*.[110] These Guidelines are designed to help ensure consumers that they are as protected when shopping online as when they buy from their local store or order from a catalogue. Their objective is to encourage (i) fair business; (ii) advertising and marketing practices; (ii) clear information about an online business identity, the goods or services it offers and the terms and conditions of any transaction; (iii) a transparent process for the confirmation of transactions; (iv) secure payment mechanisms; (v) fair, timely and affordable dispute resolution and redress; (vi) privacy protection; and (vii) consumer and business education.

Regarding online payments, Guideline V recommends that "consumers should be provided with easy-to-use, secure payment mechanisms and information on the level of security such mechanisms afford".

During the process of reviewing these Guidelines, the OECD issued the *Report on Consumer Protection in Online and Mobile Payments* and the *Consumer Policy Guidance on Mobile and Online Payments*, considering the emergence of and the need for safer and more convenient online and mobile payments.[111] The *Report* and the *Consumer Policy Guidance* identify issues that policy makers may need to address to strengthen consumer confidence in new and emerging payment platforms. They cover seven areas related to (i) clarity, transparency and completeness of the information; (ii) privacy; (iii) security; (iv) confirmation process; (v) children; (vi) fraudulent and misleading commercial practices; and (vii) dispute resolution and redress.

The BIS also develops important reports and principles related to the provision of payment services, mainly through the Committee on Payments and Market Infrastructures (CPMI).

The CPMI promotes the safety and efficiency of payment, clearing, settlement and related arrangements, thereby supporting financial stability and a wider economy. It also serves as a *forum* for central bank cooperation in related oversight, policy and operational matters, including the provision of central bank services.

The CPMI is responsible, among other issues, for monitoring and analysing developments to help identify risks for the safety and efficiency of arrangements within its mandate, as well as resulting risks for the global financial system; establishing and promoting global standards and recommendations for the regulation, oversight and practices of arrangements within its mandate, including guidance for their interpretation and implementation, where appropriate; and supporting cooperative oversight and

[110] OECD, 2000.
[111] OECD, 2012b; OECD, 2014.

cross-border information-sharing, including crisis communication and contingency planning for cross-border crisis management.

The CPMI cooperates with other standard setters (in particular the International Organization of Securities Commissions – IOSCO, and the Basel Committee on Banking Supervision), other central bank bodies (such as the Committee on the Global Financial System), international financial institutions and public sector bodies on matters falling within its mandate to enhance coordination of policy development and implementation.

In 2012 the Committee on Payment and Settlement Systems (CPSS), currently CPMI, and IOSCO issued the *Principles for Financial Market Infrastructure* (PMFI) which are applicable to payment systems in general, including internet payments.[112]

In 2014 the CPMI published the report *Non-banks in retail payments*, which analyses the role of non-banks in retail payments, including the possible implications for central banks. This report focuses on the regulatory frameworks in force to address retail payment system risks, and identifies different approaches that central banks may adopt.[113]

Self-regulation initiatives

The majority of PSPs adopt, on their own initiative, standards, principles and other supporting materials issued by international bodies working specifically in the payment systems field, such as the European Payments Council (EPC), and the PCI Security Standards Council.

The EPC is an international not-for-profit association, which represents PSPs and aims to support and promote European payments integration and development, notably the SEPA.

This Council is committed to promoting safe, reliable, efficient, convenient, economically balanced and sustainable payments, which meet the needs of payment service users and support the goals of competitiveness and innovation in an integrated European economy.

The EPC pursues this purpose through the development and management of pan-European payment schemes and the formulation of positions and proposals on European payment issues in dialogue with other stakeholders and regulators at the European level.

The PCI Security Standards Council was founded by five international brands of card schemes (American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc.) and is an open global forum responsible for the development, management, education, and awareness of the PCI Security Standards.

The PCI Security Standards Council issues standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organisations ensure the safe handling of cardholder information at every

[112] CPSS/IOSCO, 2012.
[113] BIS, 2014.

step. The keystone is the PCI Data Security Standard (PCI DSS) which provides an actionable framework for developing a robust payment card data security process, including prevention, detection and appropriate reaction to security incidents.

In addition, most PSPs build their information security management systems in accordance with requirements of the international standards issued by the International Organization for Standardization (ISO). The ISO - an independent non-governmental membership organisation - develops voluntary international standards. According to this organisation, “International Standards make things work. They give world-class specifications for products, services and systems, to ensure quality, safety and efficiency. They are instrumental in facilitating international trade”.[114]

[114] See section “Risk mitigation initiatives”.

SUPERVISORY FRAMEWORK

Key points from the survey responses

- Financial supervisory frameworks of respondent jurisdictions have significant differences as regards providers under the financial supervisory perimeter. In some jurisdictions, such as the EU countries, PSPs are under the scope of financial supervisors. In other jurisdictions, where non-financial providers have a relevant market share, financial supervisory competent authorities may have limited powers to oversee their action or no power at all since they are not under the financial supervisory perimeter.
- The responses to the survey show that ongoing collaboration among prudential supervisors, conduct of business supervisors and payment systems overseers contributes to the mitigation of security risks and to the enhancement of consumer protection.
- Some jurisdictions consider the analysis of payment service users' complaints (or the data on complaints) as one of the most powerful tools to monitor the PSPs' conduct, define or propose regulatory provisions and define supervisory actions.
- Respondent jurisdictions report that the traditional supervisory tools, such as on-site inspections and off-site monitoring, should be also used to oversee compliance by PSPs with security regulations and guidelines.
- Financial education initiatives are widely promoted in respondent jurisdictions. They include initiatives aimed at increasing the financial literacy and awareness of users, namely in regards to their rights and obligations, the risks involved in digital payment transactions and the precautions that should be observed to guarantee safe payments.

Overview

Deposit and credit institutions are facing competition from new PSPs, such as payment institutions, electronic money institutions, and MNOs in the market of innovative retail payments. The co-existence of various types of providers enhances supervisory difficulties and creates new challenges for supervisors.

According to the survey responses, not all the new PSPs are within the financial supervisory perimeter and therefore they are not subject to the supervisory and consumer protection frameworks to which regulated providers are.

A comprehensive supervisory framework should take into consideration the various, but complementary, perspectives and goals of payments supervision – prudential supervision, conduct of business supervision and payment systems oversight – and desirably be based on the sharing of information and good practices among supervisors and overseers both at national and international level.

The increasing use of innovative channels to make payments presents challenges for effective supervision and oversight. Survey respondents refer the adoption of traditional supervisory tools to

oversee online and mobile payments. Analysis of complaints, or the data on complaints, has been considered one of the most important indicators on the identification of emerging risks, and their causal drivers. This tool is used to assess compliance by PSPs with regulations, enhancing also consumer protection. On-site inspections and, in particular, off-site monitoring are also mentioned as important tools. However, the supervision of digital payments leads to a reflection about the suitability and efficiency of traditional supervisory tools. The responses to the survey confirm the relevance of this discussion.

In addition to conventional supervisory tools focused on PSPs, supervisors or other competent authorities should promote initiatives to empower users. Financial education initiatives can play an important role in understanding security risks and promoting users' awareness of their rights and obligations, and of the precautions they should observe to guarantee safe payments. These initiatives may be carried out by supervisors and by PSPs and industry and consumer associations, all of which are closer to consumers when digital payment services are used.

The scope of supervision

The responses to the survey reveal that some jurisdictions do not have a regulatory framework applicable to non-financial providers. The total amount of money involved in payment transactions made by a financial PSP may be also a criterion to exclude it from the financial supervisory perimeter.

While regulated PSPs must observe a set of provisions regarding consumer protection, unregulated providers fall outside the supervisory perimeter. The provision of payment services by PSPs that are not under the scope of financial supervision authorities may result in an increased risk of misleading or deceptive information about the costs and characteristics of the payment service.

In the EU, all payment services governed by PSD must be provided by entities subject to financial supervision. Financial supervisors oversee all PSPs under the scope of the PSD.[115]

In Brazil, the Central Bank (BCB) supervises only PSPs that may impact on systemic risk, considering the amounts involved in their payment transactions. Brazil's legal framework establishes that the payment schemes that do not impose risks that could affect the regular and adequate functioning of retail payment transactions are not subject to its provisions. Law No 12.865 of 9 October 2013, sets the general guidelines that the BCB will observe in order to determine which payment schemes fit this risk-free description, while granting the National Monetary Council (CMN) the power to determine which parameters are necessary for applying that interpretation. Therefore, according to the defined

[115] In the EU, only a very minor and specific set of payment services are outside of the scope of PSD. Hence, only in these cases, their providers fall outside of the scope of PSD. For instance, PSD is not applicable to services based on instruments that can be used to acquire goods or services only in the premises used by the issuer or under a commercial agreement with the issuer either within a limited network of service providers or for a limited range of goods or services (Article 3 (k) PSD). Meanwhile, the new PSD (PSD2) re-defines the list of services excluded from the Directive shrinking the exemptions and embracing new payment services, such as payment initiation services and account information services. Therefore, providers offering online banking-based payment initiation (third-party PSPs) will become regulated by this new regulation and their conduct will be supervised.

criteria, risk-free payment schemes are not participants in the Brazilian Payments System (SPB) and are not supervised by the BCB.

According to the legislation currently in place, the business models known as 'private labels' are not regulated by the BCB. In this specific model, payment instruments are issued by a commercial entity (e.g. department store) and are only accepted by that same retail establishment.

Moreover, based on the powers assigned by the aforementioned legislation, the BCB decided that other payment schemes with limited or specific purposes are also not subject to its regulation (e.g. schemes which set rules and procedures establishing that all issued payment instruments can only be used in a specific chain of stores, such as in franchises or licensed establishments, or to make payments in regard to the provision of public services, such as for water supply, electricity and transportation purposes).

Another criterion, related to the volume of transactions that are carried out through each payment scheme, was also taken into consideration by the BCB when determining which payment schemes are under its regulatory scope. In order not to inhibit innovation initiatives and the development of diversified business models, while preserving the security, efficiency and proper functioning of markets, it was established that small payment schemes that display volumes of transactions lower than the following requirements are also not subject to the BCB's regulation and supervision:

- R$ 500 million, taking into account the sum of all transactions that took place in the past 12 months;
- 25 million transactions, taking into account the number of transactions that took place in the past 12 months;
- R$ 50 million in resources deposited in payment accounts in a 30-day period of time, where this took place at any time over the past 12 months;
- 2.5 million active consumers in a 30-day period of time, where this took place at any time over the past 12 months.

Those values will be gradually decreased over the next few years, in order to reach 50% of their original amounts on 1 January 2018, and 10% on 1 January 2019.

Taking into consideration the various different players in this market, the BCB is working together with telecommunications supervisors taking into consideration the various different players in this market. Since 2013, the BCB, the Ministry of Communications and Brazil's telecommunications regulator have been, by law, expected to work together to enable the telecommunications sector to offer payment services and foster financial inclusion in Brazil.

A collaborative supervisory approach

The supervision of online and mobile PSPs implies, due to the idiosyncrasies of this innovative market, a close cooperation among supervisors and overseers. Where and when relevant cooperation with non-financial supervisors may also be considered.

At the EU level, the implementation by each country of EBA *Guidelines on the security of internet payments* may be considered a good example of cooperation among prudential supervision, conduct of business supervision and payment systems oversight.[116]

Prudential supervisors are responsible for supervising PSPs' compliance with the security requirements related to risk control, incident monitoring and mitigation risks, in order to ensure the security of PSPs' payment systems. Supervisors should ensure that PSPs implement an effective internal risk control and incident reporting policy concerning online and mobile payments, whose objective is to ensure their financial stability and the safety of the funds entrusted to them. The purpose of prudential supervision is to safeguard the security of payments in each PSP and the security of the financial payment system, with the overall objective of ensuring financial stability.

According to the EBA Guidelines, PSPs should implement and regularly review a formal security policy for internet payment services and carry out and document thorough risk assessments with regard to the security of internet payments and related services. PSPs should also implement security measures in line with their respective security policies in order to mitigate identified risks.

The EBA Guidelines also focus on customer awareness, education and communication, establishing that PSPs should provide assistance and guidance to customers, where needed, with regards to the secure use of the internet payment services. The implementation of an accurate security policy by PSPs contributes to the protection of payment service users; PSPs should provide one secured channel for ongoing communication with customers regarding the correct and secure use of the internet payment service, and to promote customer education and awareness initiatives.

The provision of a secure channel by PSPs may also be considered an important conduct of business security requirement that provides protected communication between each customer and her/his PSP. Through this channel, users are informed about updates in security procedures and significant emerging risks regarding internet payment services. Ultimately, the enhancement of users' awareness about security measures aims to ensure the execution of payment transactions in a secure manner, thus contributing to the fight against payment fraud and the enhancement of consumer confidence in internet payments.

The supervision of PSPs' compliance with these security requirements may fall under the scope of conduct of business supervision, given that the main objective is the improvement of consumer protection, namely the prevention of losses. Moreover, these security requirements also take into consideration the relationship between customers and PSPs.

The creation and implementation of a security policy must also be defined in line with payment systems oversight. Indeed, overseers should monitor the PSPs' payment systems and assess whether their implemented solutions allow the efficient and effective processing of transactions in a secure environment.

[116] The proposed reflection may be not fully adjusted to all EU jurisdictions, due to the differences regarding division of competences among national competent authorities. For instance, in Portugal, an internal group was set up with members from the Banking Prudential Supervision Department, the Banking Conduct Supervision Department and the Payment Systems Department to ensure the PSPs' compliance with the EBA Guidelines.

Payment systems oversight should evaluate whether the technical solutions implemented by PSPs in order to achieve the prudential requirements ensure the proper and secure functioning of payment systems, and the correct and timely processing of transactions.

Cooperation between supervisors and overseers is essential for: the proper, efficient and secure functioning of payment systems; ensuring that PSPs have adequate mechanisms to assess risks of online and mobile payment services and prevent their emergence; and guaranteeing that PSPs have installed the proper hardware and software to control and mitigate risks, and that customers trust the security of online and mobile payments. Permanent collaboration among prudential supervisors, business conduct supervisors and payment systems overseers can thus help improve consumer protection. When conduct of business supervision is conducted by an authority other than the central bank, a very close collaboration should be established.

Supervisory activities rely essentially on domestic supervisors. However, an international exchange of information and sharing of good supervisory practices between supervisors is crucial due to the particularities of innovative payments, namely their cross-border nature.

Supervisory tools

Based on the survey responses, it is possible to conclude that supervisors are using traditional supervisory tools, such as management of complaints, on-site inspections and off-site monitoring, and data analysis, to monitor and oversee PSPs. The efficiency of these traditional tools to oversee digital payments should be assessed by supervisors.

Management of complaints

The management of complaints from payment service users is an important supervisory tool. It plays a crucial role in the field of innovative payments, helping supervisors to closely monitor the payment service market by identifying the most significant security risks related to those services. Data from complaints also allow supervisors to keep track of developments on payment services supply and customers' main concerns, enabling a closer oversight of PSPs conduct of business.[117]

Complaints can be used as a tool to ensure that PSPs are complying with regulatory security requirements, ceasing irregular practices, preventing the re-occurrence of infringements, and identifying gaps in the regulatory framework. The complaints analysis provides supervisors with significant data to propose the adoption of regulatory conduct of business provisions to remedy the identified gaps.

[117] In accordance with Article 99 (1) of PSD2, "Member States shall ensure that procedures are set up which allow payment service users and other interested parties including consumer associations, to submit complaints to the competent authorities with regard to PSPs' alleged infringements of this Directive". It seems that the EU legislator recognises the management of complaints as an important supervisory tool, which allows the monitoring of the payments market and increases consumer protection.

In addition, information collected through complaints can be used to plan inspections, off-site monitoring of priorities and key objectives, and to develop financial education programmes. The handling of complaints can also contribute to the identification of systemic misconduct flaws and, as such, it is crucial to ensure financial stability.

In some jurisdictions, the supervisory authority collects, registers and analyses complaints from payment service users regarding the conduct of financial PSPs. In other countries, the supervisory authority only collects data on complaints made against financial PSPs. In both frameworks, the supervisory authority may then take proper measures in case of infringements of the regulatory framework and within the scope of its responsibilities.

Case study: Portuguese complaints handling process

In Portugal, the management of complaints is an important supervisory tool. The Central Bank registers and analyses all the complaints that are sent directly by customers or which are recorded in the *Complaints Book*, which must be made available upon request by every credit institution, financial company, payment institution and electronic money institution. The right to complain may be exercised by any individual or company that is a user of a PSP.

Supervised entities are required to analyse all the users' complaints and to inform the user and the Central Bank of the result of their analysis. The Central Bank receives this information and analyses the complaints in order to assess compliance by the entity with the regulatory framework. In addition, should the Central Bank need additional information about the complaint during the analysis, supervised entities must cooperate with the Central Bank and give the requested information. If the Central Bank concludes that the entity did not comply with the applicable legislation or regulation, it takes the necessary measures to ensure compliance by the entity with those provisions and informs the user of the result of its analysis.

The Central Bank analyses all the complaints within the scope of its legal responsibilities. However, the intervention of the Bank does not cover the resolution of strictly contractual issues between PSPs and their customers, since the resolution of these disputes, when an agreement is not reached, requires the intervention of judicial or arbitral entities. Moreover, any matter related to poor service falls under social conduct principles, and, therefore, does not fall under the Central Bank's scope of action.

The Central Bank publishes an annual report that covers all the analysed complaints. The report identifies the main subjects of complaints, ranks the institutions by the number of complaints regarding each subject, the complaint's status and the analysis result.

In Brazil, the supervisory authority (BCB) receives complaints against financial institutions and seeks to ascertain whether there was evidence of non-compliance with legal and regulatory provisions, the enforcement of which is BCB's responsibility. In this jurisdiction, the monitoring of complaints is also an important supervisory tool, helping the supervisory authority to supervise and regulate the activities of financial institutions and define financial education policies. In addition, complaints with evidence of irregularity, not removed after hearing arguments from the financial institutions, are used in forming the ranking of institutions by complaints index.

In its survey response, the Indonesian Financial Services Authority (IFSA) reported having 'Financial Consumer Care' to handle any financial complaints. This system provides a function called 'Traceable', for financial institutions, and another function called 'Trackable', for consumers. The

'Trackable' application gives consumers access to the system to check the progress of their complaints, while 'Traceable' gives financial institutions access to information and to take the necessary action to resolve the complaint before the Indonesia IFSA takes any action on it.

This is also the practice in Philippines, where the Central Bank receives complaints from financial consumers against supervised financial institutions and assists in the resolution of complaints by facilitating the communication between said parties. The Central Bank also keeps track of the complaints, inquiries and requests received from the public and analyses the issues to determine the policies needed to uphold consumer protection.

In Japan, the Financial Service Agency (JFSA) has a 'Counselling Office for Financial Services Users' that responds to general questions, to requests and feedback from financial service customers concerning financial administration and financial services. Expert counsellors respond to the questions and requests by phone. Furthermore, the feedback from customers is shared by other sections in the JFSA and is used to promote consumer protection. The Office cannot mediate or accommodate a dispute, but places advisors in institutions, as appropriate, to respond to the problem, or summarises the issue based on advisory activities. The JFSA publishes counselling data and a summary every quarter. It also publishes case studies of problems that customers have faced. These examples are useful for other financial customers in managing such problems.

In Canada, the Financial Consumer Agency of Canada (FCAC) also collects complaints and breach reports related to the provisions for which it is responsible. In general, these focus on supervising compliance with the Bank Act of Canada, which may refer marginally to, but does not explicitly focus on, online or mobile payments.

In the UK and Ireland, the supervisory authority receives data on complaints from the Ombudsman, an independent and impartial entity that deals with consumers' complaints regarding the provision of financial services.

In the UK, the supervisory authority collects and publishes data on complaints made against firms in two formats: at the individual firm level and at an aggregate (total) level. Data on complaints are published on the FCA's website every six months and helps the FCA to monitor how individual firms are handling consumer complaints, and also highlights any emerging issues or risks. The FCA's rules do not require firms to report a complaint if it is resolved by the close of business on the business day after the complaint is received.

In Ireland, the Central Bank also collects data on complaints, namely complaints data for each payment service (e.g. bank accounts, payment cards, etc.), but does not collect data on complaints related to mobile or online use of payment instruments. The Central Bank uses these data to identify whether any trends are developing in the market which may lead to consumer detriment or are indicative of poor behaviour towards consumers.

In Australia, the supervisory authority (ASIC) receives and considers reports of misconduct, breach reports from licensed entities, and carries out surveillance to check compliance with the financial services laws where appropriate. ASIC has a range of compulsory powers to acquire information to support the surveillance of the supervised entities for ensuring compliance and investigation of breaches of legislation. ASIC does not generally publish statistics on reports of misconduct or assist in the resolution of individual complaints.

In addition to the management of complaints, some respondent jurisdictions also make Alternative Dispute Resolution (ADR) procedures available to payment service users.

ADR procedures (such as conciliation, arbitration and mediation) allow payment service users to resolve their disputes with PSPs out-of-court. Typically, users submit the dispute to a neutral third party (the ADR entity or ombudsman) who acts as an intermediary between them and the PSPs. The ADR entity can suggest or impose a solution to the dispute, or simply bring the user and the PSPs together to discuss how to find a solution. ADR procedures are usually quicker, simpler and less expensive than courts (and may be free of charge).

The EU legislator issued two important legal acts regarding the ADR procedures, to ensure better consumer protection and therefore boost confidence in the internal market.

Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 aims to allow customers access to simple, efficient, fast and low-cost ways of resolving domestic and cross-border disputes which arise from sales or service contracts.

The Directive establishes that EU Member States should facilitate access by consumers to ADR procedures and embraces a set of requirements applicable to ADR entities and ADR procedures. According to the Directive, ADR entities notified to the EU Commission by Member States should offer a high quality service and respect core principles, such as impartiality, transparency, effectiveness and fairness.

The Directive provides the legal basis for ADR as a whole. Its requirements are applicable to ADR entities responsible for the settlement of contractual disputes in virtually all economic sectors apart from the location of the trader (domestically or cross-border) and the type of transaction (online and offline).[118]

Considering the growth of e-commerce and the lack of adequate consumer protection regarding disputes arising from online purchases, the EU legislator also issued **Regulation (EU) No 524/2013** of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes.

“The purpose of this Regulation is, through the achievement of a high level of consumer protection, to contribute to the proper functioning of the internal market, and in particular of its digital dimension by providing a European ODR platform (‘ODR platform’) facilitating the independent, impartial, transparent, effective, fast and fair out-of-court resolution of disputes between consumers and traders online.” [119]

Developed and operated by the EC, the ODR platform facilitates the online resolution of contractual disputes stemming from online sales or service contracts between a consumer resident in the EU and a trader established in the EU, through the intervention of an ADR entity. The list of ADR entities is published on the ODR platform.

[118] EC, 2016.
[119] Article 1 of the Regulation.

This new regulation embraces the provision of online payment services, enhancing the protection of online payment service users. The ODR platform aims to be user-friendly and is multilingual.

To submit a complaint to the ODR platform, the consumer should fill in an online complaint form and submit it. Documents in support of the complaint may be attached. The complaint is sent to the relevant trader, who proposes an ADR entity to the consumer. Once consumer and trader agree on an ADR entity to handle their dispute, the ODR platform transfers the complaint automatically to that entity. The ADR procedure should be concluded within 90 days.

The regulation establishes a set of obligations to traders regarding consumer information. Traders established within the EU engaging in online sales or service contracts should provide on their websites an electronic link to the ODR platform, which should be easily accessible for consumers. Traders who have chosen or are obliged to use one or more ADR entities to resolve disputes with consumers should also inform consumers about the existence of the ODR platform and the possibility of using the ODR platform for resolving their disputes and provide an electronic link to the ODR platform in the offer, when it is made by email.

Given the importance of ADR procedures to enhance consumer protection, the **Payment Services Directive** has already established that EU Member States should ensure that adequate redress procedures for the settlement of disputes between payment service users and PSPs are put in place for disputes concerning rights and obligations arising under the scope of this Directive. The new Payment Services Directive reinforces the role of ADR procedures, establishing that PSPs should also inform the payment service user about at least one ADR entity which is competent to deal with disputes concerning the rights and obligations arising under Titles III and IV of the Directive.

On-site inspections and off-site monitoring

On-site inspections and off-site monitoring are the most common supervisory tools used in several jurisdictions. They were mentioned in the survey responses of Armenia, Brazil, China, France, Ireland, Japan, Norway, Portugal, and Saudi Arabia, either as part of a themed inspection or as reactive inspections in response to specific concerns.

On-site inspections and off-site monitoring allow the assessment of PSPs' compliance with the regulatory framework, in particular in what respects disclosure of information and security requirements, and the identification of the commercial practices of supervised entities.

On-site inspections are performed (i) directly at PSPs' head offices, by accessing their systems and available information (such as internal procedures); (ii) at their branches as accredited inspections, where inspectors analyse samples of operations or collect relevant documentation; or (iii) at their branches through mystery shopping, where unidentified inspectors play a role, acting like customers interested in one or more payment services and asking for information about them. The purpose of mystery shopping is usually the evaluation of the information given to customers (transparency, completeness, etc.). A mixed strategy may also take place, i.e., a mystery shopping inspection may evolve later to an on-site identified inspection (accredited inspection).

Off-site monitoring does not involve direct interaction with the supervised PSPs. The target in this case is the information publicly available on websites and in advertising campaigns, and the information regularly reported to the supervisory authority.

In Portugal, mystery shopping plays an important role in the Central Bank's banking conduct supervision strategy. It is a valuable instrument for assessing compliance with the legal and regulatory framework applicable to the provision of payment services because it allows an effective assessment of how products and services are being sold to customers, and an evaluation of the market conduct of PSPs, regarding, for example, selling practices, information disclosure and the duty of assistance. The Central Bank also develops off-site monitoring through the analysis of information available on the PSPs' websites and data reported by PSPs (such as price lists).

In Ireland, inspections performed by the Central Bank of Ireland have focused on some financial entities' technology and business continuity plans in order to mitigate the risk of IT outages, security of those entities' systems, timeliness and quality of consumer communications when outages or other issues occur, and redress in appropriate cases.

Data analysis

The analysis of data reported by PSPs is also an important supervisory tool, allowing supervisors to obtain relevant information about the functioning of payment systems, and the PSPs' commercial practices. Supervisors can obtain this information in several ways; in some jurisdictions, PSPs are required to report periodic information on advertising, contracts or fraud losses to the supervisor.

In Ireland, the Consumer Protection Code requires financial entities to report any errors to the Central Bank of Ireland that have caused loss or delay to consumers. Bank IT outage or unauthorised persons gaining access to banking systems and overcharging for online payment services are some examples of errors which would impact the effectiveness of online or mobile payment services and which should be reported to and monitored by the Central Bank. The Central Bank of Ireland also requires those institutions to put a communications plan in place in order to ensure that consumers are informed during the outage. The Central Bank then monitors these issues to ensure that they are resolved in a timely manner and any affected consumers are appropriately redressed. Furthermore, in 2013 the Central Bank of Ireland implemented online conduct of business returns, requiring institutions to provide data on their sales and complaints on a half yearly basis. This allows the Bank to identify any trends which might lead to consumer detriment or are indicative of poor behaviour towards consumers.

The new PSD2 also establishes that, in the case of a major operational or security incident, PSPs shall, without undue delay, notify the competent authority in the home Member State of the PSP. Where the incident has or may have an impact on the financial interest of its payment service users, the PSP shall, without undue delay, inform its payment service users of the incident and of all measures that they can take to mitigate the adverse effects of the incident.[120] This rule illustrates the importance of cooperation and exchange of information between prudential and conduct of business supervisors.

In some jurisdictions, surveys of PSPs may also be used to gather information on compliance with the regulatory framework.

In Japan, the supervisory competent authority (JFSA) regularly reviews the procedures on whether

[120] Article 96.

each financial institution properly addresses fraudulent online transfers, such as unauthorised withdrawal of deposits, based on regular updates from each institution. In addition, the JFSA conducts an annual survey in order to get a clear picture of the security measures that have been implemented by each financial institution, for instance, whether a variable password or an electronic certificate has been put in place.

Furthermore, the JFSA regularly modifies ‘Guidelines for Supervision’ and ’Operational Guidelines’ which provide the area which needs to be focused on home banking services and conducts supervisory activities and on-site inspections based on the Guidelines and "Inspection manual".

Enforcement powers

Supervisory authorities are usually given the powers to enforce the regulatory framework. These powers contribute to an effective application of the regulatory framework of PSPs.

In general, the enforcement powers include the issuing of penalties and sanctions, in particular administrative fines, and also the power to issue specific orders in case of non-compliance with the regulatory framework. The competent authority may adopt a specific measure, depending on the frequency and the severity of the infringement.

In Japan, for example, the competent authority is authorised to order service providers to improve or suspend their business, and to revoke their license or registration. Moreover, juridical criminal penalties can be imposed on service providers that violate regulatory acts.

According to the Irish survey response, the Central Bank has statutory powers to take administrative action against any regulated financial service provider offering online and mobile payment services.

Similarly, in Portugal, the Central Bank has enforcement powers. The Central Bank issues specific orders and recommendations requiring PSPs to correct detected irregularities. The Bank also has the power to initiate administrative proceedings in the event of infringement and to impose sanctions and ancillary penalties.

In Canada, the competent authority (FCAC), as a regulatory agency, can exercise its enforcement powers to ensure that federally regulated financial entities comply with the consumer provisions of the various federal acts relating to financial services, including the Bank Act, the Co-operative Credit Associations Act, the Payment Card Networks Act, and the Financial Consumer Agency of Canada Act. In cases of contravention or non-compliance with the legislation, the FCAC notifies the federally regulated financial entity of a violation and may also, depending on the severity and frequency of the problem, adopt different measures such as aim for a commitment from the financial entity to remedy the issue within a short time, impose a monetary penalty or criminal sanctions and take other action if necessary.

Similarly, in the UK, the FCA has a wide range of enforcement powers including fines, warnings, banning powers and both civil and criminal prosecution powers. The FCA’s approach to enforcement is based on ‘a credible deterrence’ strategy that aims at deterring future malpractice by taking tough and public action against firms and individuals that fail to comply with the regulatory framework.

In South Africa, both the South African Reserve Bank (SARB) and the Payments Association of South Africa (PASA) have enforcement powers. PASA’s powers allow it to sanction the conduct of PASA’s

Members (banks and designated non-banks) that are in contravention of rules issued by the SARB and PASA.

Financial education initiatives

Payment service users with financial literacy competences can make better decisions regarding mitigation of security risks in digital payment services. Users need to be more aware of the security risks related to these payment services and of the importance of meeting security requirements implemented by PSPs to mitigate those risks, even if they reduce the convenience of the digital payments. Campaigns targeted to users to raise awareness of the need to comply with security requirements play a crucial role.

As an example, at the EU level, the EBA issued Guidelines on the security of internet payments that should be observed by national supervisors and PSPs. Guideline 7 establishes that "the initiation of internet payments, as well as access to sensitive payment data, should be protected by strong customer authentication". According to this guideline, PSPs "should have a strong customer authentication procedure", i.e., a "procedure based on the use of two or more of the following elements – categorised as knowledge, ownership and inherence: i) something only the user knows, e.g. static password, code, personal identification number; ii) something only the user possesses, e.g. token, smart card, mobile phone; iii) something the user is, e.g. biometric characteristic, such as a fingerprint. In addition, the elements selected must be mutually independent, i.e. the breach of one does not compromise the other(s). At least one of the elements should be non-reusable and non-replicable (except for inherence), and not capable of being surreptitiously stolen via the internet. The strong authentication procedure should be designed in such a way as to protect the confidentiality of the authentication data".

In order to comply with this Guideline, PSPs must gain the cooperation of users, because the adoption of strong customer authentication implies a more demanding authentication and, consequently, a more time-consuming process. Accordingly, users should be aware of and familiar with these procedures, and be informed about new security measures.

The majority of survey respondent jurisdictions recognise the importance of financial education of users regarding the mitigation of security risks, referring to the promotion of their own initiatives or of those being included in national financial education strategies, typically developed by financial market authorities and the government. There are also jurisdictions reporting that even when a national financial education strategy is not in place, national authorities are developing initiatives with information about the positive and negative aspects that consumers should be aware of when using digital payment services.

Spain and Canada mentioned that the national financial education strategy includes topics on online and mobile payment services. In Saudi Arabia, the increase of consumer awareness regarding innovative payments has also been identified as a key strategic priority for the Saudi Arabian Monetary Agency.

The Central Bank of Brazil designed the 'Financial Citizenship Programme' aligned to the national strategy for financial education, which aims at promoting financial education and access to information about the financial system, including information on security risks associated with online and mobile payments. Additionally, the Central Bank has a strategic partnership with the National Consumer

Protection Secretariat, linked to the Ministry of Justice, which develops initiatives that also address security risks on online and mobile payments.

In Japan, the 'Report of Study Group on Financial Education' by Study Group on Financial Education which is established under the Financial Research Center of the Financial Services Agency (JFSA), published in April 2013, is included in Japan's national strategy. Based on this, the 'Council for Financial and Economic Education Promotion', composed of JFSA and related institutions, published the 'Financial Literacy Map' in 2014 that clarifies and systematises 'minimum financial literacy' skills by items and ages. For online and mobile payment skills, there are a few topics that need to be acquired, such as, if people know examples of online fraud and understand the necessity to be aware of them, and if consumers can implement security countermeasures. Moreover, the JFSA is cooperating with relevant ministries to raise awareness among payment providers of the need to strengthen their security, and to direct customers' attention towards this matter.

National financial education strategies commonly include the development of specific content for websites, covering information about the advantages, the security risks associated with and the precautions that must be taken while using online and mobile payment services. That is the case of Portugal, Canada, France, Armenia, Ireland and Indonesia.

In Portugal, the Central Bank has developed relevant content for the *Portal do Cliente Bancário* (Bank Customer Website) on the major security issues related to online and mobile payment services and instruments. This website is managed by the Central Bank under the remit of its mandate on banking conduct supervision. Similar information was also developed by the Central Bank for the *Todos Contam* (Everybody counts) website under the national plan for financial education.

In Canada, national authorities have also included alerts on the security risks of online and mobile commerce and payments on their websites. Among those authorities are FCAC, which has developed content on online banking, including consumer information on accessing accounts online using a computer or mobile device and tips for protecting financial information online (complementary content for mobile payments is also being developed); the Government of Canada, which has developed the website *Get cyber safe*, focused on cyber security from various personal perspectives including financial aspects; and the Office of the Privacy Commissioner, which has the website '*Youth privacy*' with resources and tools to advise young people about the relevance and importance of privacy when using digital technologies.

The French national financial education strategy also has an educational website, *La finance pour tous*, informing the public on banking and financial topics, and the *abe-infoservice* website of the Autorité de Contrôle Prudentiel et de Résolution informing customers about preventive measures and issuing alerts on online and mobile payment risks. Furthermore, the Central Bank of France distributes brochures that inform consumers about the security risks of payment forms that include online payments.

In Armenia, the national strategy on financial education covers security risk issues associated with online and mobile payments, included in the theme 'Management of personal financial risks and understanding how to safely use financial instruments (avoiding fraud and forgery)'. A special section on 'online shopping and payment' is also included in the financial educational website (*'abcfinance'*) of the Central Bank of the Republic of Armenia, which has information on the security risks of online and mobile payments.

In Ireland, the Competition and Consumer Protection Commission promotes consumer awareness by publishing information on their *Consumer help* website in order to educate consumers about financial products and services, or to warn them of any issues that could have a detrimental impact.

The Indonesian Financial Services Authority has relevant publications on its website, informing consumers about safety issues of online and mobile payments and has launched a mobile app (called *Yuk Sikapi*) to reach out to internet and smartphone users on financial education matters, including the topic of online and mobile payment services.

The Luxembourg Government manages a website (*BEE-Secure*) that aims to inform people about the safe use of information and communication technologies and contains a section dedicated to risks associated to e-banking and online banking.

From the survey responses it was also possible to identify a number of initiatives that involved holding seminars and/or training sessions for payment service customers with a focus on the security risks related to online and mobile payment services.

This is the case, for example, of Lithuania, where the Bank of Lithuania aims to reach a wider target audience and therefore holds several initiatives on online payments for senior citizens and students in schools, including online video seminars.

In Portugal, the Central Bank is developing, under the national financial education strategy, training sessions focused on digital payments, and in particular on their advantages, risks and security measures. These training sessions are being developed with different target audiences, namely students and teachers.

The Armenian survey response also revealed that information on the security risks associated with online and mobile payments is available in materials used on seminars catering to different target groups, such as the army, people living in rural areas, and students.

In South Africa, the consumer education department of the Financial Services Board performs a number of activities to inform consumers about scams and safety with their money and identity, which include workshops and exhibitions via a website, a call centre and face-to-face presentations.

The survey response from the Indonesian FSA has also stated that they have issued press releases to inform consumers to take precautionary steps in ensuring the safety of online and mobile transactions, namely regarding the use of technology.

The Central Bank of the Philippines also holds events to promote financial education, the Financial Education Expo (Fin-Ed Expo), in different parts of the country, to inform the public about the available financial tools to help in the promotion of their financial well-being. Likewise, they also hold Financial Empowerment Seminars (FES) to familiarise the public with banking institutions and their products and services and distribute related reading materials.

For the development of a financial education initiative, supervisors may benefit from the research of international organisations dedicated to financial education. The importance of digital financial services is by now recognised and debated by the major international forums, namely by the OECD/INFE.

CONCLUSIONS

Developments in the payments market are based on technological upgrades of conventional payment services and instruments. In many cases, the **new online and mobile payment service** is the traditional service with different and innovative features.

The digitalisation of payments markets comes with **new PSPs** that are taking a lead role in this evolution. Traditionally delivered only by deposit and credit institutions, new payment services are currently also being developed by new types of financial institutions and, often, by institutions acting in the non-financial sector (e.g. telecommunications companies, retailers, or transport companies). Banks face fierce competition from new players, forcing them to invest intensely in new technological solutions. Different providers competing in this new market explain the expansion of more and more innovative services through alternative channels. The continuous evolution of both services and providers is promoting a fruitful cycle of innovation.

The combination of innovative payment services and new providers is bringing **new risks, in particular security risks,** to the payments market. Fraudulent transactions affect consumer trust in digital payment services. Payment service users should also be adequately protected against deceptive practices, such as subscription traps and practices of 'cramming'.

The ongoing diversity and complexity of new online and mobile payments is **challenging financial regulators and supervisors**. The regulatory framework and the supervisory approach to online and mobile payments and providers should closely focus on technological developments and on the continued emergence of new services and PSPs to be able to address and mitigate the potential impact of risks they may bring. Regulatory gaps need to be overcome and adequate supervisory tools implemented. Regulatory frameworks and supervisory tools need to permanently adjust to the new features of these payments. Supervisors should also promote awareness campaigns regarding the safe use of new payment services.

The traditional consumer protection framework is being tested and **supervisors** are often caught behind new market trends. Given the increasing use of online and mobile payments and the emergence of new security risks, supervisors should bear in mind that a comprehensive consumer protection approach should embrace specific tools to mitigate these risks. Furthermore, issues related to disclosure of information and deceptive commercial practices are also among those that may require a new supervisory approach. A flexible and dynamic supervisory framework is required. It should impose on PSPs the provision of guidance and assistance to users of digital payments. Moreover, supervised entities may be required, when appropriate, to identify the traditional payment service behind the innovative payment service offered, in which channels this service is available, the risks involved, and how consumers can mitigate the risks.

New digital PSPs may be small entities, and therefore perceived as not implying high systemic risk. Supervisors may be tempted to underestimate their action. However, they may also affect trust in the financial system. The close monitoring of the digital payments market is particularly important to supervisors not only from the consumer protection perspective, but also as a systemic risk threat. Besides involving relevant issues on an individual basis, security incidents may have potential impact for **systemic risk**.

Finally, it should be underlined that the entrance of new payment services in the market can also affect its **integrity** and efficiency. A close cooperation among prudential supervisors, conduct of

business supervisors and overseers will contribute to define a comprehensive policy of supervision and oversight, allowing the enhancing of consumer protection, financial stability and efficiency of payment systems.

Besides the challenges related to the increasing use of digital payments at a national level, supervisors should also take into consideration that these new payment services are easily accessible, allowing cross-border flows. The cross-border movement of funds through digital channels raises new issues to supervisors, which are able to compromise the enhancing of consumer protection and the prevention of money laundering and terrorist financing. The cross-border provision of payment services requires strong **international dialogue and cooperation** among the different relevant *fora*.

FinCoNet wishes to play a role in promoting the discussion at an international level of supervisory challenges brought about by the new digital economic system. It intends to reflect on these important issues under the consumer protection umbrella to promote a greater understanding of the risks and development of effective supervisory tools. FinCoNet also acknowledges the importance of developing awareness campaigns to increase financial literacy on digital financial services. FinCoNet wants to discuss these matters with all relevant international organisations and is keen to promote cross-border cooperation across jurisdictions taking into consideration internationalisation of online and mobile payment services. Thus, this report aims to be an input to foster discussion among international *fora*.

APPENDIX – RESPONDENT JURISDICTIONS

Jurisdiction	Respondent
Armenia	Central Bank of Armenia
Australia	Australian Securities and Investments Commission
Austria	Financial Market Authority
Brazil	Central Bank of Brazil
Bulgaria	Bulgarian National Bank
Canada	Financial Consumer Agency of Canada
Chile	Superintendencia de Bancos e Instituciones Financieras
China	People's Bank of China
Estonia	Estonian Financial Supervision Authority
France	Autorité de Contrôle Prudentiel et de Résolution
Indonesia	Indonesia Financial Services Authority
Ireland	Central Bank of Ireland
Japan	Financial Services Agency
Latvia	Consumer Rights Protection Centre of Republic of Latvia
Lithuania	Bank of Lithuania
Luxembourg	Commission de Surveillance du Secteur Financier
Macedonia	National Bank of the Republic of Macedonia
Netherlands	Authority for the Financial Markets
Norway	The Financial Supervisory Authority of Norway
Philippines	Central Bank of the Republic of the Philippines
Poland	National Bank of Poland
Portugal	Bank of Portugal
Saudi Arabia	Saudi Arabian Monetary Agency
South Africa	South African Reserve Bank / Financial Services Board
Spain	Bank of Spain
Swaziland	Financial Services Regulatory Authority
United Kingdom	Financial Conduct Authority

GLOSSARY

Term	Definition
App	Short for 'application', which refers to a small, specialised programme that is downloaded on mobile devices for a specific purpose.
Bluetooth	Wireless technology standard for exchanging data between fixed and/or mobile devices over short distances. Data transmission is based on a special radio frequency that creates a short range network.
CNP (Card-Not-Present Payment)	Transactions made with no face-to-face contact between the cardholder and the merchant, no tangible payment card to inspect for security features, and no physical signature on a sales draft to check against the card signature, such as payments made via internet, post or telephone.
Cramming	Charges added to a phone bill by a third party without the subscriber´s permission.
Deposit and credit institutions	Financial institutions that are legally allowed to take deposits or other repayable funds from the public and to grant credits for their own account.
Digital wallet	Procedures agreed between the provider and the consumer to initiate a payment from linked payment cards or accounts, which can be accessed through devices connected to the internet or through mobile communication systems (such as NFC and Bluetooth). It can be incorporated in banking tools made available to the consumer by their deposit/credit institution, or offered by a third party.
Direct mobile billing	Purchase charges placed directly on a bill (commonly a mobile phone bill), for example, as payment for downloaded digital content through a mobile phone.
EBPP (Electronic Bill Presentment and Payment)	Process by which companies send bills to their customers and receive their payments electronically over the internet, or other electronic method.

Term	Definition
EMV	International technical standard, developed by Europay, MasterCard and Visa (EMV), for payment cards equipped with a processor chip ('chip and PIN cards' or 'chip and signature cards'), and for payment terminals and ATMs which accept them. Payment cards can be 'contact cards' which are physically inserted into a reader, or 'contactless cards' which are read over NFC technology.
G20	Group of 19 countries plus the EU, representing both developed and emerging economies whose size or strategic importance gives them a particularly crucial role in the global economy (http://www.oecd.org/g20/about.htm).
GSM (Global System for Mobile Communications)	Standard developed by the European Telecommunications Standards Institute (ETSI) to define the protocols for second-generation (2G) digital mobile networks used by mobile phones.
Home banking	Banking services accessed via the internet.
Malware	Malicious software designed to disrupt devices' normal functioning, gather personal data or obtain access to private computer systems.
Money remittance	Transfer of funds received from a payer, without any bank or payment account, to a payee or to another PSP acting on behalf of the payee. Money remittance most often refers to funds sent by a foreigner to an individual in her / his home country.
NFC (Near Field Communication)	Short-range, contactless communication system, based on Radio Frequency Identification (RFID) technology that allows payment data transfer between devices.
Payment instruments	Any personalised device(s) and/or set of procedures agreed between the payment service user and the PSP and used by the payment service user to initiate a payment transaction (e.g. payment cards, home banking security credentials).
Payment services	Activities that include, namely (i) services enabling cash to be placed on a payment account; (ii) services enabling cash withdrawals from a payment account; (iii) execution of direct debits; (iv) execution of payment transactions through a payment card or a similar device; (v) execution of credit transfers; and (vi) money remittance.

Term	Definition
Profiling	Aggregation of large amounts of user data, enabling the identification of users' habits, interests and other personal information.
Payment transactions	Acts, initiated by the payer or by the payee, of placing, transferring or withdrawing funds, irrespective of any underlying obligations between the payer and the payee.
Pharming	Fraudulent method that occurs when a provider's URL is hijacked and the user is redirected to a fake site, or when fake apps are provided on mobile devices.
Phishing	Fraudulent method to acquire sensitive personal data, such as usernames, passwords, and security credentials, by masquerading as a reputable entity, a website or email in order to lure the user.
Phone phishing (or vishing)	Fraudulent method that consists of using the telephone system to gain access to personal and financial information from users for the purpose of financial reward.
QR-Code	Two-dimensional barcode, consisting of black modules arranged on a white squared background, which can be linked to text, URL or other data. The code is readable by mobile devices with appropriate QR-code readers.
RIFD (Radio Frequency Identification)	Wireless technology that consists of electromagnetic fields which transfer electronically stored data, between a small chip and an antenna/reader, serving the same purpose as bar codes or magnetic stripes.
SIM Card	Subscriber Identity Module Card. Refers to a small card used in a mobile phone to store data of user identity, location and phone number, network authorisation data, personal security keys, contact lists and stored text messages. It includes security features such as authentication and encryption to protect data.
SIM card swap	Fraudulent method that occurs when users' mobile phone is attacked and the incoming phone calls and SMS are received by a SIM card in the fraudster's possession.

Term	Definition
Smishing (SMS phishing)	Fraudulent method that consists of sending a text message to an individual's mobile phone in an attempt to get her/him to provide relevant personal and financial data.
USSD (Unstructured Supplementary Service Data)	Protocol used by Global System for Mobile Communications (GSM) mobile phones to communicate with the network provider's system. It is used as part of the configuration of the phone on the network and allows WAP browsing, prepaid call-back service, mobile-money services, location-based content services, menu-based information services. Unlike SMS, USSD messages create a real-time connection during a USSD session, which remains open and allows a two-way exchange of a sequence of data.
Vishing (phone phishing)	Fraudulent method that consists of using the telephone system to gain access to personal and financial information from users for the purpose of financial reward.

REFERENCES

AFI (Alliance for Financial Inclusion) (2014), *Mobile Financial Services: Consumer Protection in Mobile Financial Services*. Available at http://www.afi-global.org/sites/default/files/publications/mfswg_guideline_note_7_consumer_protection_in_mfs.pdf

BIS (2012), Committee on Payment and Settlement Systems (CPSS), *Innovations in retail payments*. Available at http://www.bis.org/cpmi/publ/d102.pdf

BIS (2014), Committee on Payments and Market Infrastructures (CPMI), *Non-banks in retail payments*. Available at http://www.bis.org/cpmi/publ/d118.pdf

CGAP (Consultative Group to Assist the Poor) (2015), *Doing Digital Finance Right: The Case for Stronger Mitigation of Customer Risks*. Available at http://www.cgap.org/sites/default/files/Focus-Note-Doing-Digital-Finance-Right-Jun-2015.pdf

Consumers International (2014), *Mobile payments and consumer protection*. Available at http://www.consumersinternational.org/media/1439190/ci_mobilepaymentsbriefing_jan14_final.pdf

EBA (2014), *Final guidelines on the security of internet payments*. Available at http://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1

EC (2012), *Green Paper: Towards an integrated European market for card, internet and mobile payments*. Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0941:FIN:EN:PDF

EC (2015), *A Digital Single Market Strategy for Europe - Analysis and Evidence* (Commission Staff Working Document). Available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&from=EN

EC (2015a), *Green Paper on retail financial services: better products, more choice, and greater opportunities for consumers and business*. Available at: https://ec.europa.eu/transparency/regdoc/rep/1/2015/EN/1-2015-630-EN-F1-1.PDF

EC (2016), *Settling consumer disputes online* (Factsheet). Available at http://ec.europa.eu/consumers/solving_consumer_disputes/docs/adr-odr.factsheet_web.pdf

ECB (2010), *Single Euro Payments Area: Seventh progress report – Beyond theory into practice*. Available at https://www.ecb.europa.eu/pub/pdf/other/singleeuropaymentsarea201010en.pdf

ECB (2013a), *Recommendations for the security of internet payments*. Available at https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf

ECB (2013b), *Recommendations for the security of mobile payments – draft document for public consultation*. Available at https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf?7f9004f1cbbec932447c1db2c84fc4e9

ECB (2015), *Fourth report on card fraud*. Available at https://www.ecb.europa.eu/pub/pdf/other/4th_card_fraud_report.en.pdf

EMC – RSA, The Security Division of EMC (2009) *Phishing, Vishing and Smishing: old threats present new risks*. Available at http://www.emc.com/collateral/white-papers/h11933-wp-phishing-vishing-smishing.pdf

ENISA (European Union Agency for Network and Information Security) (2014), *Network and Information Security in the Finance Sector*. Available at http://www.enisa.europa.eu/activities/Resilience-and-CIIP/nis-in-finance/network-and-information-security-in-the-finance-sector

EP (2015), *Consumer protection aspects of mobile payments*. Available at http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564354

Europol (European Police Office) (2015), Europol website: The Internet Organised Crime Threat Assessment. Available at https://www.europol.europa.eu/iocta/2014/chap-3-6-view1.html

FBI (Federal Bureau of Investigation) (2015), FBI website: Scams & Safety – Common Fraud Schemes. Available at https://www.fbi.gov/scams-safety/fraud (Accessed: 3 September 2015).

FCA (Financial Conduct Authority) (2013), *Mobile banking and payments: Supporting an innovative and secure market*. Available at http://www.fca.org.uk/static/documents/thematic-reviews/tr13-06.pdf

FCA (2014), *Mobile banking and payments*. Available at http://www.fca.org.uk/static/documents/thematic-reviews/tr14-15.pdf

FCA (2015), *Business Plan 2015/16*. Available at http://fca.org.uk/static/channel-page/business-plan/business-plan-2015-16.html?utm_source=businessplan2015&utm_medium=businessplan2015&utm_campaign=businessplan2015#c1

FCAC (2013) (Financial Consumer Agency of Canada), *Mobile Payments and Consumer Protection in Canada*. Available at http://www.fcac-acfc.gc.ca/Eng/resources/researchSurveys/Documents/FCAC_Mobile_Payments_Consumer_Protection_accessible_EN.pdf

FCAC (2015), *International Review: Mobile Payments and Consumer Protection*. Available at http://www.fcac-acfc.gc.ca/Eng/resources/researchSurveys/Documents/InternationalReviewMobilePaymentsAndConsumerProtection.pdf

FED (Federal Reserve System) (2015), *Consumers and Mobile Financial Services 2015*, Washington, DC. Available at http://www.federalreserve.gov/econresdata/consumers-and-mobile-financial-services-report-201503.pdf

Flatraaker, Dag-Inge (2013), *Mobile payments changing the landscape of retail banking: Hype or reality?*, Journal of Payments Strategy & Systems.

G20/GPFI (2014), *Issues Paper: Digital Financial Inclusion and the Implications for Customers, Regulators, Supervisors and Standard-Setting Bodies*.

Hadnagy, Christopher and Fincher, Michele(2015), *Phishing dark waters – The offensive and defensive sides of malicious Emails*, Indianapolis: Wiley.

Hayashi, Fumiko (2012), *Mobile Payments: What's in It for Consumers?*, Federal Reserve Bank of Kansas City, Economic Review – First Quarter 2012. Available at https://www.kansascityfed.org/~/media/files/publicat/econrev/econrevarchive/2012/1q12hayashi.pdf

King, Brett (2012, October 10), *'Generation M': The Emergence of "See and Hear" Brand Engagement*, The Huffington Post. Available at http://www.huffingtonpost.com/brett-king/generation-m-see-and-hear_b_1946776.html (Accessed: 14 September 2015).

King, Brett (2013), *Bank 3.0*, Singapore: Marshall Cavendish Business.

King, Brett (2014), *Breaking Banks – The innovators, rogues, and strategists rebooting banking*, Singapore: Wiley.

Krishnan, Sankar (2014), *The power of mobile banking*, New Jersey: Wiley.

Lieber, Ron (2014), *The Most Serious Threat When Using Credit: You*, The New York Times, 10 October 2014. Available at http://www.nytimes.com/2014/10/11/your-money/the-slippery-plastic-slope-to-overspending.html?_r=0

Mayer-Schönberger, Viktor, and Cukier, Kenneth (2013), *Big Data*, John Murray Publishers.

OECD (2000), *Guidelines for Consumer Protection in the Context of Electronic Commerce*. Available at http://www.oecd.org/sti/consumer/34023811.pdf

OECD (2010), *Consumer Policy Toolkit*. Available at http://www.oecd.org/sti/consumer/consumer-policy-toolkit-9789264079663-en.htm

OECD (2011), *G20 High Level Principles on Financial Consumer Protection*. Available at http://www.oecd.org/daf/fin/financial-markets/48892010.pdf

OECD (2012a), *Presentation at the FinCoNet special workshop on financial inclusion, mobile banking and consumer protection*.

OECD (2012b), *Report on Consumer Protection in Online and Mobile Payments*. Available at http://www.oecd-ilibrary.org/docserver/download/5k9490gwp7f3.pdf?expires=1420818065&id=id&accname=guest&checksum=45C26866AA0A1CCBF084CA83040D8E8B

OECD (2014), *Consumer Policy Guidance on Mobile and Online Payments*. Available at http://www.oecd-ilibrary.org/science-and-technology/consumer-policy-guidance-on-mobile-and-online-payments_5jz432cl1ns7-en

PCI SSC (Payment Card Industry – Security Standards Council) (2015) website. Available at https://www.pcisecuritystandards.org/organization_info/index.php (Accessed: 7 September 2015).

Skinner, Chris (2014), *Digital bank*, Singapore: Marshall Cavendish Business.

Sterling, Toby (2015, April 17), *Europol Director: hackers target banks, not customers*, Reuters. Available at http://www.reuters.com/article/2015/04/17/us-europol-cybersecurity-idUSKBN0N81RN20150417 (Accessed: 14 September 2015)

Thaler, Richard H. (2015), *The making of behavioural economics*, Allen Lane.

World Bank (2012), *Innovation in retail payments worldwide: a snapshot*. Available at http://siteresources.worldbank.org/financialsector/resources/282044-1323805522895/innovations_in_retail_payments_worldwide_consultative_report(10-17).pdf

World Bank (2015), *The Global Findex Database 2014 – Measuring financial inclusion around the World*. Available at http://www.worldbank.org/en/programs/globalfindex