Online and mobile payments

An overview of supervisory practices to mitigate security risks

January 2018

Acknowledgements

The International Financial Consumer Protection Organisation (FinCoNet) would like to acknowledge the efforts of Standing Committee 3 in developing this project and bringing it to a conclusion. Standing Committee 3 consists of representatives from Australia, Brazil, Canada, China, Indonesia, Japan, Mauritius, Portugal, South Africa and the United Kingdom and is supported by staff from the OECD Secretariat. In particular, we would like to thank Maria Lúcia Leitão as Chair of the Standing Committee as well as Agus Fajri Zam, Andréia Lais de Melo Silva Vargas, Carla Ferreira, Caroline da Silva, Christian Groves, Claire Lawrie, David Pereira, Francisco Silveira, Hiroko Suzuki, Hudiyanto, Inês Póvoa, Kosuke Ito, Miho Tanaka, Patrícia Guerra, Rudi Saleh Susetyo, Sam Stoakes, Shaoshua Zhang, Sitaresmi Purnamasari, Sofia Duarte, Stanislaw Zmitrowicz, Steve Trites, Teresa Frick, Tiandu Wang, Tilotma Gobin Jhurry and Xiaoxiao Li for their work in writing and producing the survey and report.

FinCoNet would also like to express its full appreciation to all respondents to the *Questionnaire for conduct of business supervisors – Mitigating security risks with actions proposed in the FinCoNet report 'Online and mobile payments: supervisory challenges to mitigate security risks'*.

About FinCoNet

FinCoNet was established in 2003 as an informal network to enable discussions among financial consumer protection regulators and supervisors regarding consumer protection issues of common interest. It is recognised by the Financial Stability Board and the G20.

In November 2013, FinCoNet was formally established 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

1. Executive Summary 9

Background 9

Overview of the questionnaire 13

Purpose of this report 13

2. Conduct of Business Supervisory Practices 15

Challenge 1 - Adequate legal and regulatory framework

- Scope 15
- Main findings from the questionnaire's responses 15
- Supervisory practices 16

Challenge 2 - Ongoing and comprehensive monitoring of the main risks

- Scope 21
- Main findings from the questionnaire's responses 21
- Supervisory practices 22

Challenge 3 - Close cooperation between supervisors and other relevant entities

- Scope 29
- Main findings from the questionnaire's responses 30
- Supervisory practices 31

Challenge 4 - Close supervision of PSP's disclosure of information

- Scope 42
- Main findings from the questionnaire's responses 43
- Supervisory practices 43

Challenge 5 - Ongoing assessment of security risks through supervisory tools

- Scope 47

- Main findings from the questionnaire's responses 47
- Supervisory practices 48

Challenge 6 - Promotion of awareness campaigns on security risks

- Scope 52
- Main findings from the questionnaire's responses 52
- Supervisory practices 53

Challenge 7 - Promotion of digital financial literacy

- Scope 58
- Main findings from the questionnaire's responses 59
- Supervisory practices 60

3. **Key Takeaways** 64
4. **Annex I - Respondents** 66
5. **Annex II - Questionnaire** 68

Graphs

Graph 1 Adequate legal and regulatory framework 15

Graph 2 Ongoing and comprehensive monitoring of the main risks 21

Graph 3 Close cooperation between supervisors and other relevant entities 30

Graph 4 Close supervision of PSPs' disclosure of information 43

Graph 5 Ongoing assessment of security risks through supervisory tools 47

Graph 6 Promotion of awareness campaigns on security risks 52

Graph 7 Promotion of digital financial literacy 59

Tables

Table 1 Conduct of business supervisory challenges, approaches and examples of actions to mitigate security risks raised by digital payments 11

Table 2 Platforms for exchanging information and/or reacting to security incidents 34

Figures

Figure 1 Established partnerships at national level. 34

Figure 2 Ilustration of international fora where payments or security issues are discussed 36

Table of acronyms and abbreviations

App	Application
CERT	Computer Emergency Response Team
CNP	Card Not Present
CPMI	Committee on Payments and Market Infrastructures
CSIRT	Computer Security Incident Response Team
EBA	European Banking Authority
EC	European Commission
ECB	European Central Bank
EP	European Parliament
EU	European Union
FinCoNet	International Financial Consumer Protection Organisation
FinTech	Financial Technology
GPFI	Global Partnership for Financial Inclusion
GDPR	General Data Protection Regulation
IT	Information Technology
KID	Key Information Document
MoU	Memorandum of Understanding
NIS	Security of Network and Information Systems
OECD	The Organisation for Economic Co-operation and Development
PIN	Personal Identification Number
PSD	(EU) Payment Services Directive
PSP	Payment Service Provider
RTS	Regulatory Technical Standards
SC3	FinCoNet Standing Committee 3
SupTech	Supervision Technology

1. EXECUTIVE SUMMARY

Background

FinCoNet committed to examining the fast-paced development of technological innovation in the provision of payment services to consumers – in particular security risks as a threat to consumer protection.

In September 2016, FinCoNet released the report prepared by Standing Committee 3 (SC3), *Online and mobile payments: supervisory challenges to mitigate security risks* [1]. The report focuses on how regulators and supervisors are responding to emerging risks raised by digital payments, with special emphasis on security risks, and recognises how they are keeping up with the pace of innovation, while looking at issues to increase consumer trust and confidence in the digital ecosystem. It also identifies and sets out next steps for further work for FinCoNet to carry out on this topic, highlighting a set of challenges and identifying approaches that conduct of business supervisors may use to mitigate security risks, including examples of actions to be taken by supervisors.

Later in November 2016, the comprehensive analysis presented in the report was discussed by FinCoNet members at their Annual General Meeting in Jakarta [2]. FinCoNet members agreed on the 2017/2018 FinCoNet's programme of work [3] and instructed SC3 to continue working on online and mobile payments by giving the Committee a mandate to monitor the implementation of approaches and actions in response to the identified challenges.

It was also decided that given the fact that digital services can easily be accessed across borders, the "Survey on cross-border transactions" [4] conducted by Japan's Financial Services Agency would be included in SC3's further work.

Members stressed the importance of fostering collaboration between FinCoNet and relevant international *fora* to widen the discussion regarding digital payment services under the consumer protection umbrella to intensify cross-border cooperation among jurisdictions.

While implementing its mandate, SC3 promoted a worldwide discussion with FinCoNet observers and other international *fora.* As an outcome of this cooperation, the additional challenge ("having an adequate legal and regulatory framework in order to foster effective supervision") proposed by the World Bank was included as part of the work (Table 1). This challenge was acknowledged as the foundation of an effective supervision of digital payments, allowing the implementation of actions to tackle the challenges identified.

SC3 developed a questionnaire to identify specific actions being adopted by conduct of business supervisors to mitigate security risks in the digital ecosystem falling under the scope of the challenges

[1] Available at http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf.
[2] For more information, see http://www.finconet.org/2016finconetannualgeneralmeeting.htm.
[3] See http://www.finconet.org/FinCoNet_communique_on_priorities-2017.pdf.
[4] Available at http://www.finconet.org/Cross_Border_Transactions-Summary_Responses.pdf.

listed in the 2016 report. The draft questionnaire was presented and discussed at the FinCoNet Seminar and Open Meeting on 7 April 2017 in Dublin [5].

[5] For more information, see http://www.finconet.org/finconetopenmeeting2017.htm.

Table 1 Conduct of business **supervisory challenges**, approaches and examples of actions to mitigate security risks raised by digital payments

Supervisory challenges	Supervisory approach	Examples of actions to be taken
Challenge 1		
• **Having an adequate legal and regulatory framework to foster effective supervision**	• Supervisors should incorporate in their actions the provision of online and mobile payments, given their new risks and features and the fast pace at which they are evolving	• Developing a specific risk-based supervision methodology for online and mobile payment services, considering the particularities of these services (e.g. high quantity of transactions, and small amounts involved) • Using innovation and technology – including SupTech – for effective and efficient supervision
Challenge 2		
• **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, 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)
Challenge 3		
• **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
Challenge 4		
• **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 therefrom 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

Challenge 5		
• **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, which could include the identification of regulatory gaps**	• 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
Challenge 6		
• **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 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
Challenge 7		
• **Coordinated approach between conduct of business supervisors and national bodies responsible for financial literacy to promote the use of precautionary procedures for digital customers**	• Supervisors may maintain close collaboration with financial literacy bodies to further promote precautionary attitudes and safety procedures for 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 for users (e.g. strong customer authentication)

Overview of the questionnaire

The questionnaire was crafted to collect information on supervisory practices or initiatives to mitigate security risks in the digital ecosystem. In June 2017, SC3 distributed it to several supervisory authorities in various jurisdictions. The distribution list included FinCoNet Members and non-Members, as well as international bodies.

The questionnaire consisted of a set of "yes or no" questions and an optional "in progress" column for actions implemented or pending. Respondents were also tasked to provide detailed descriptions of specific initiatives or experiences and to describe other relevant initiatives related to each challenge. Respondents were invited to suggest any practice/initiative/line of action that should be highlighted as case studies of supervisory initiatives to mitigate security risks in the digital ecosystem falling within the scope of different challenges. (To view the questionnaire, please see Annex II).

The questionnaire aimed to identify supervisory actions with a peer-learning purpose. It did not have comparative or evaluation purposes; instead it provided an opportunity for respondents to share initiatives and experiences.

SC3 was pleased to receive the important contribution of 32 responses from different jurisdictions and continents; 21 responses from FinCoNet Members and Observers and 11 from other jurisdictions and international organisations.

Purpose of this report

The analysis presented in this report is based on responses to the *Questionnaire for conduct of business supervisors – Mitigating security risks with actions proposed in the FinCoNet report, 'Online and mobile payments: supervisory challenges to mitigate security risks'.* [6]

The report aims to:

(i) provide an analysis of the questionnaire responses regarding conduct of business supervisory initiatives to tackle the challenges identified in the 2016 Report, *Online and mobile payments: supervisory challenges to mitigate security risks*;

(ii) present the conduct of business supervisory practices or initiatives identified within each challenge that are being implemented across jurisdictions to mitigate security risks in the digital context; and

(iii) highlight specific lines of action being used to address the distinct features and risks of online and mobile payments.

The report is organised in three sections: (1) executive summary, (2) conduct of business supervisory practices and (3) key takeaways.

[6] In this regard, some changes to the submitted "yes", "no" or "in progress" answers were needed considering the corresponding supporting comments presented.

The executive summary includes a background, the overview of the questionnaire and the purpose of the report. The second section is organised by challenge, with an introduction, explaining each one's scope, followed by a quantitative assessment of the main findings of the questionnaire's responses, and examples of supervisory practices adopted by respondents.[7] The last section summarizes the main conclusions of this report.

The overriding goal of this report is to provide supervisors a meaningful resource for their reflections and decisions on approaches and policies to tackle security risks posed by digital payments.

By implementing this project FinCoNet acknowledges the importance of ongoing and comprehensive monitoring of the digital payment services market, taking into consideration its specific features and risks. In this fast-changing and global ecosystem, close cooperation among conduct of business supervisors, prudential supervisors, payment systems overseers and other relevant entities, at the national and international level, is considered crucial.

FinCoNet also highlights that conduct of business supervisors should actively participate or encourage a digital financial strategy to promote the implementation of security mechanisms by PSPs and the adoption of precautionary measures by payment service users.

[7] Annex I lists the Questionnaire's respondents and Annex II presents the corresponding layout.

2. CONDUCT OF BUSINESS SUPERVISORY PRACTICES

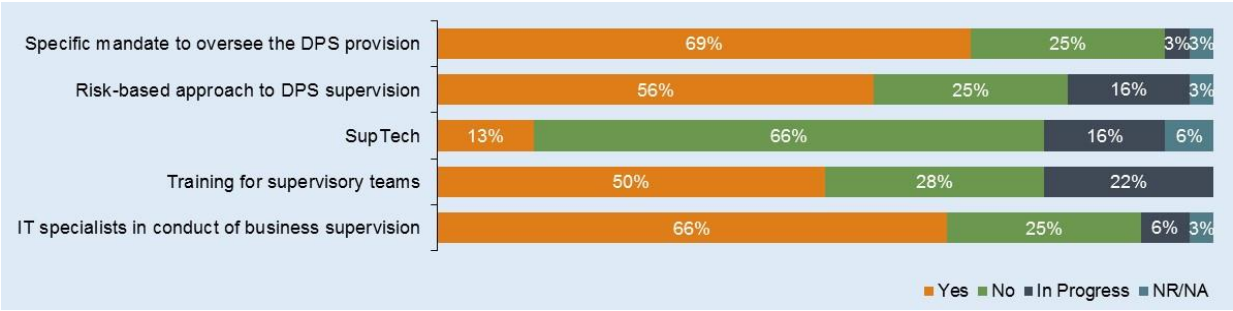
Challenge 1	Having an adequate legal and regulatory framework to foster effective supervision

Scope

- A legal and regulatory framework is crucial to protect financial consumers and foster effective supervision. It should outline a wide set of rules covering all financial services and products, including payments. Given the risks these services and products present to consumers – security being the most significant – payment services also require a clear set of principles and rules.
- To be effective, conduct of business supervisors should receive an explicit mandate, on the basis of which and together with other authorities would oversee the mitigation of security risks.
- Supervisors should develop a specific risk-based methodology, taking into account products and services' features, and possess innovative tools (SupTech) for an effective and efficient supervisory process.
- Supervisory teams whose mission is the oversight of digital payment services should receive specific training to keep up with technology and innovation development and to be able to identify the risks arising from these services.
- Conduct of business supervisors should also be able to make use of IT specialists to enhance their functions while overseeing digital payment services.

Main findings from the questionnaire's responses

Graph 1 Adequate legal and regulatory framework [8]



[8] See Annex II for the complete set of questions included under this topic in the questionnaire.

- The majority of respondents reported that they had been granted, either generically or specifically, a mandate to oversee the provision of digital payments. It is unclear, however, whether the answers refer to the specific conduct of business supervisory mandate.
- A risk-based approach to supervision is followed by most of the jurisdictions. Some mentioned that they apply a specific approach to digital payment services.
- Most of the respondents do not use innovation and technology (SupTech[9]) in supervision to mitigate security risks, although some countries indicated they were progressing in that direction. Only a few use technology as an oversight tool.
- Supervisors recognise the importance of specific IT training for teams responsible for overseeing digital payments. Most of them provide training for their supervisory teams – although often not in a systematic way – or will do so.
- IT specialists are working in conduct of business supervision in most of the jurisdictions. Some supervisors are able to assign IT teams from other departments to conduct of business supervision. A couple of respondents recognised the importance of including IT specialists in the future.

Supervisory practices

A specific mandate to oversee the provision of digital payment services

In some jurisdictions, such as Brazil, Ireland and Portugal, conduct of business supervisors are responsible for overseeing the provision of digital payments. In other countries, a mandate to supervise digital payments is conducted only under the scope of prudential supervision.

A specific risk-based approach to supervise digital payment services

In Spain, the Central Bank currently follows a general risk-based approach in the conduct of business supervision to identify the risk profile of each supervised entity. To that end, the supervisor considers a set of variables, including types of payment services. France focuses on practices that could represent higher risk to consumers.

In Singapore, legislation confers information-gathering and regulatory powers on the Monetary Authority of Singapore (MAS). In particular, MAS may designate and regulate the payment systems relevant to the stability of the financial system, particularly those that are considered systemically important, of system-wide relevant or where there is a public interest to do so.

[9] SupTech refers to the application and use of innovative or cutting-edge technology by supervisors to carry out their supervisory and surveillance work more effectively and efficiently (*e.g.* big data usage, machine learning).

A proactive approach to the supervision of digital payments in Canada

In Canada, at the federal level, the Financial Consumer Agency of Canada (FCAC) proactively monitors, identifies and evaluates trends and emerging issues, including in digital payments that may have an impact on consumers of financial products and services. Various tools and data can be used for this activity such as complaints data, internal assessments, interviews, and public reports.

FCAC is also contributing to the federal government's work to develop an oversight framework for retail payments to promote a well-functioning payments system that fosters innovation and better protects consumers. This work is being led by the Department of Finance and a consultation paper will be published in 2017. Based on the results of its consultations, the Government will propose legislation to implement the oversight framework.

The Autorité des Marchés Financiers (AMF) also takes a proactive approach to the supervision of digital payments. Operational risk supervisors are regularly looking for online and mobile payments solutions being developed by financial institutions and other organisations. Incidents, trends and alerts on payment technology from different sources and social media are identified and shared among the supervision specialists and managed when needed. Every financial institution must notify the supervisor when a major incident takes place.

Use of innovation and technology (SupTech) to mitigate security risks

France and the Netherlands are using technology (SupTech) to mitigate security risks. The Bank of France[10] has a specialised unit in charge of the security issues related to payment services, using oversight tools such as online and automated (fulfilment of) quantitative and qualitative annual assessments.

Prioritisation of investment in technology as a way to strengthen supervision in the Netherlands

The Dutch Authority for the Financial Markets (AFM) has been prioritising investment in technology and methodologies to strengthen and renew supervision. In particular, the AFM aims to improve insight into consumer behaviour and the conduct of financial enterprises and audit firms. Also noteworthy is the set-up of the AFM's Expertise Center in 2016 to invest in further knowledge accumulation and sharing, and promoting technological and methodological innovation within the organisation. In this context, the AFM started the "Spot-on programme" with the aim of increasing the organisation's skills in relation to data management and analysis. It was foreseen that in 2017, this programme would support the transition to a data-driven supervisory authority and improve supervision by facilitating data research and the development of a data and analysis platform.

[10] For practical reasons, the names of central banks are in English.

According to the supervisor, with this platform the institution is "building a safe, sustainable and future-proof environment that allows for the use of data in primary supervision in a modern, flexible and user-friendly manner". It should be noted, though, that the supervisor does not use this technology specifically to prevent or mitigate security risks of digital payment services.

Specific training for the supervisory team responsible for digital payments

In some jurisdictions, like Chile, Estonia and Portugal, supervisors give (or have given) their teams the opportunity to participate in international events, training sessions and workgroups to learn, and share information and best practices among conduct of business supervisors. In the same vein, Macedonia promotes visits with other supervisors so the corresponding teams learn from external experiences. In some countries such as Ireland and Portugal, supervisors also share information among different areas/departments within the same organisation, leveraging on internal expertise.

IT specialists working in conduct of business supervision

In some countries such as Macedonia, Mozambique and Portugal, IT experts are working in conduct of business supervision. In Germany, supervisors benefit from a cross-section IT area. The German Federal Financial Supervisory Authority (BaFin) has a department dedicated to IT supervision. The department includes IT specialists, economists and lawyers, all working closely together. Canada and Ireland reported leveraging general internal IT resources or requesting IT support from other departments.

An inclusive model of supervision in Peru[11]

In Peru, digital payment services can be provided by financial institutions and the Electronic Money Issuing Entities (EEDE).

Both entities – financial institutions and EEDE – are under the Superintendency of Banks, Insurance and Pension Funds' (SBS) regulatory perimeter, which has the mandate to oversee the provision of digital payment services.

EEDE, in particular, were created with the main purpose of electronic money issuance, not granting credit based on funds received and only allowed to carry out operations related to their main purpose. The SBS issues regulations covering the main aspects of these enterprises, such as corporate purpose, authorisation to operate, and application of prudential measures.

[11] Law No 29985 ("Ley del Dinero Electrónico") and Díaz, Conde, "Modelo Peru – Unique Model, Unique Challenges, Bright Future", 2017, available at https://www.iif.com/publication/research-note/modelo-peru-unique-model-unique-challenges-bright-future

A particular feature of these enterprises is that they use telecommunication services to operate, allowing the execution of digital payments through mobile phones. As such, the telecommunications regulator, OSIPTEL, establishes the provisions that guarantee access to the telecommunication services by those financial companies.

This framework helped pave the way for the development of an inclusive model – *Modelo Perú* – where financial institutions, telecommunication companies and other stakeholders cooperate to design a platform that aims to take financial services to remote areas and reduce transaction costs. According to Global Microscope (2016), it includes all the major players in the financial system, and customers can make transactions through phone companies.[12]

Special Task Force for Financial Innovation in Poland

In January 2017, the Polish Financial Supervision Authority (KNF), together with the Ministries of Finance and Development, formed a Special Task Force for Financial Innovation in Poland involving other supervisors, regulators and market participants (both regulated and start-ups) to develop solutions to mitigate legal and supervisory barriers to FinTech growth. The Task Force deals with about 100 barriers, identified by market participants, to FinTech growth in Poland. The final outcome of the work will be a report in which the regulatory and supervisory barriers to the development of the FinTech sector in Poland will be presented. The report will also include proposals for possible actions on the side of the competent authorities. The Task Force tries to eliminate as many barriers as possible on an ongoing basis (e.g. by proposing regulatory changes in the ongoing legislative processes).

The Central Bank of Ireland launched a Discussion Paper on the *Consumer Protection Code and the Digitalisation of Financial Services*

The Central Bank of Ireland conducted a public consultation on the *Consumer Protection Code and the Digitalisation of Financial Services*[13] (June 2017) to assess how consumers are protected in this environment, if the risks emerging from digitalisation are adequately addressed and whether there are impediments in the Code that

[12] http://www.centerforfinancialinclusion.org/storage/documents/EIU_Microscope_2016_English_web.pdf

[13] https://centralbank.ie/docs/default-source/publications/discussion-papers/discussion-paper-7/discussion-paper-7-digitalisation-and-consumer-protection-code.pdf?sfvrsn=0.pdf?sfvrsn=0

currently prevent firms from adopting technologies that could benefit consumers.

The Discussion Paper focuses on the areas of the above-mentioned Code that follow stages of the consumer journey with a regulated firm, in particular: requirements regarding access; provision of information and suitability requirements; complaints handling requirements and retention of consumer records/record keeping requirements. The central bank is seeking views on (i) whether consumers are adequately protected under existing consumer protection rules in the Code; (ii) whether this Code needs to be enhanced in specific areas; and (iii) whether it contains impediments to firms adopting technologies that could benefit consumers.

The Central Bank of Ireland aims to seek views from consumers, regulated financial services firms, FinTech firms and any other interested parties, on how consumers are or should be better protected in an increasingly digital financial services environment.

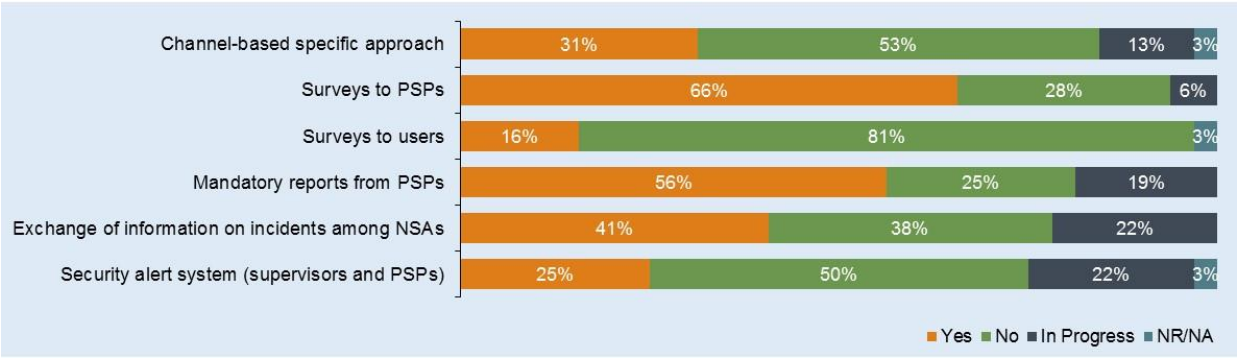
Challenge 2 Ongoing and comprehensive monitoring of the main risks related to innovative payment services

Scope

- Security concerns are a relevant barrier to the use of digital payments by consumers. Users' lack of confidence hinders increase in consumer take-up of digital payments. While fulfilling their responsibility to oversee the provision of payment services in a context of a continuous growth of innovative payments, conduct of business supervisors must closely monitor new features of digital payments and ensure that PSPs implement security risk mitigation measures.
- The assessment by conduct of business supervisors of the development of payment services and their main security incidents by channel may be an effective supervisory initiative. The adoption of a channel-based approach is relevant as the security risks raised are different given the channel used and considering that the measures to efficiently mitigate them may also be different.
- The information on security incidents is not, in the majority of cases, provided by PSPs directly to conduct of business supervisors. However, conduct of business supervisors must be aware that such information is relevant to comply with its new task to ensure the implementation of risk mitigation measures by PSPs in its relation to consumers.
- The ongoing monitoring of innovative payment services and associated risks by conduct of business supervisors should rely on up-to-date information from PSPs and users, on the regular sharing of information with prudential supervisors and payments overseers, as well as on strong collaborations with foreign and international authorities.

Main findings from the questionnaire's responses

Graph 2 Ongoing and comprehensive monitoring of the main risks[14]



[14] Please see Annex II for the complete set of questions included under this topic in the questionnaire.

- Some jurisdictions reported that when monitoring the payments market, they take into consideration whether or not payment services are being provided through digital channels, thus adopting a channel-based approach. The majority of respondents are in the process of implementing this kind of approach. A risk-based approach, an approach linked with the payment instrument (cards, credit transfers, direct debits, etc.) or a case-by-case approach that weighs the severity of incidents, are other options considered by some jurisdictions.
- The launching of surveys targeted to PSPs to monitor security risks and the adoption of precautionary measures to mitigate them is an action stated by the majority of jurisdictions.
- Surveys targeted to payment service users on security risks and the adoption of safety measures is not a common practice. Only four respondents reported this practice.
- The requirement of mandatory reports from PSPs on security incidents is a practice that a relevant number of respondents have reported. In some jurisdictions, these reports are required, but not on a mandatory or regular basis. However, from a cross-cutting analysis of the survey responses and the applicable legislation in several jurisdictions, these reports are typically required by payment overseers and prudential supervisors.
- A regular exchange of information on security incidents among national supervisory authorities (financial and non-financial sectors) is reported to be promoted by the majority of jurisdictions.
- A security alert system between supervisors and PSPs is implemented in some jurisdictions, according to the questionnaire responses. Other jurisdictions referred to recent developments in the implementation of a security alert system between supervisors and PSPs and a few reported the existence of an informal alert system.

Supervisory practices

Supervisory approaches when monitoring security incidents

When monitoring major security incidents, some jurisdictions such as Angola, Luxembourg, Mauritius and Portugal reported having a specific approach depending on the channel used.

Guidelines on Internet Banking and on Mobile Banking and Mobile Payment Systems in Mauritius

The *Guidelines on Internet Banking* (February 2001) state that "an institution operating a communicative or transactional website shall report to the Bank of Mauritius on its performance in achieving the objectives set out in its strategic and business plans, including a brief overview of its risk management processes respecting Internet banking. It shall submit to the Bank copies of its security programme and contingency and business resumption plans at the end of each financial year […]." Also, "each institution shall establish a written policy in the overall security of its Internet banking system". The Internet Banking Guidelines also establish that "each institution should ensure that the products and services offered on the Internet are fairly and accurately disclosed", including

"the features of the products and services, terms and conditions including any fees, charges, penalties and relevant interest rates".

The Guidelines on Mobile Banking and Mobile Payment Systems (February 2013, revised May 2015) establish that service providers shall submit to the Bank of Mauritius a detailed description of the entire mobile payment business process, comprising, for instance: "fund movement and settlement process"; "customer registration, services and dispute resolution mechanisms"; "information to be disclosed to the customers"; "fees and charges to be applied", etc. Moreover, the mobile PSPs shall conform to a range of processes related to "Customer Registration", "Activation", "Transaction Processing", "Settlement", "Technology and Security", "Authentication", "Modularity of Technologies", "Message Format", "Reliability", and "Security". Also, "Periodic information security audits and penetration tests of the system must be carried out" and shall include, for example: "password guessing and cracking", "carrying out regular penetration testing on the mobile payment system", and "ensuring that physical access controls are strictly enforced".

The competent authorities in Canada and South Africa mentioned that they employed a risk-based approach when monitoring major security incidents.

Surveys to PSPs on security risks

In several jurisdictions, such as Brazil, France, Germany, Poland, Portugal and Slovakia, the supervisory authority launches surveys on security risks to PSPs. The Bank of France produces an annual qualitative report. This is part of a general risk framework that is based on an annual survey of risks reported by PSPs to the Autorité de Contrôle Prudentiel et de Résolution. In December 2016, the Central Bank of Portugal launched its first questionnaire to financial institutions on banking products and services provided through digital channels.

Questionnaire on banking products and services on digital channels in Portugal

The Central Bank of Portugal launched its first 'Questionnaire on banking products and services through digital channels', in December 2016. The questionnaire was sent to the main financial institutions operating in Portugal, representing more than 95 percent of total bank deposit accounts and consumer loan contracts in the country.

The Questionnaire's goals were to assess the development of digital financial services in Portugal, the levels of adoption and use by customers, the constraints and obstacles to the demand for digital channels, and the main risks associated with the provision of financial services through digital channels and the mechanisms put in place to mitigate them. This questionnaire was organised into the following sections: (i) "Development of digital channels"; (ii) "Current accounts" aimed at identifying the functionalities available through digital channels and the main obstacles to the development of digital channels in the process of opening a bank account; (iii) "Consumer credit" aimed at identifying the features available through digital channels in the consumer loan process and main obstacles to further digitalisation; (iv) "Payment services" aimed at identifying payment

services available in digital channels and the main barriers to their development; and (v) "Security" aimed at identifying the security risks and the mechanisms in place to mitigate them.

Almost 90 percent of the financial institutions surveyed provide banking products and services to consumers online. The provision through APPs is less frequent, but more than half of the financial institutions already offer this channel to individual customers and about 29 percent plan to do so in the future.

In terms of security, the three main risks related to the use of digital channels identified were phishing, identity theft and malware. Turning to the identification of functionalities implemented by financial institutions to mitigate security risks, the following were identified: time-out for session inactivity, validation of transactions via token and encryption of communication.

The results of this questionnaire are presented in the Banking Conduct Supervision Report (2016) and in a brochure about the financial products and services provided through digital channels in Portugal.[15]

Surveys to users on security risks

In the United Kingdom, the Financial Conduct Authority (FCA) includes questions on security risks and precautionary measures adopted by users in a wider annual survey targeted to consumers.

Mandatory reports on security incidents from PSPs

In Armenia, banks are required to report on fraud incidents (phishing, counterfeit/skimming, card-not-present fraud, etc.) However, payment institutions are not formally obligated to report on security incidents. In Indonesia, the Bank of Indonesia requires PSPs to provide incidental reports in the event of network failure, fraud, and DC/DRC[16] failure of its payment system regulations. In Japan, the Financial Services Agency (FSA) requires PSPs to report major security incidents and can also require information on the security management system, if necessary. In Luxembourg, the Commission de Surveillance du Secteur Financier (CSSF) requires information on security incidents to PSPs and the PSPs, falling under the prudential supervision of the European Central Bank (ECB) (Significant Institutions) are also required to report cybercrime incidents to the ECB. In addition, the CSSF is informed of such incidents. In Peru, the supervisory authority, which adopts a risk-based approach, requires PSPs to maintain all the security incidents on its "loss event database for operational risk" and, when the security incident involves

[15] http://clientebancario.bportugal.pt/SiteCollectionDocuments/QuestCanaisDigitais2016_EN.pdf
[16] "DC/DRC" stands for "Disaster Center / Disaster Recovery Center".

significant operational interruption or a financial loss, it has to be reported to the supervisor. In South Korea, according to the Electronic Financial Transactions Act, financial companies and electronic financial business entities are responsible for analysing and assessing their electronic financial infrastructures, and reporting the findings to the supervisor at least once a year.

The Central Bank of the Republic of the Philippines is developing reporting templates that will help the core IT Specialist Group (CITSG) measure and evaluate the level of IT risk within the industry.

Exchange of information on security incidents among supervisory authorities

The exchange of information between financial and non-financial authorities is promoted, for instance, in the context of the National Strategic Framework for Cyberspace Security. Some authorities share information on security incidents with their jurisdictions cyber security agency or authority.

MoU for cooperation among national supervisory authorities in Indonesia

In Indonesia, exchange of information on security incidents is done through cooperation among national supervisory authorities in accordance with a Memorandum of Understanding (MoU). The Bank of Indonesia (BI) cooperates with several supervisory authorities, such as the Indonesian Financial Transaction Reports and Analysis Center (regarding information exchange on Prevention and Eradication of Money Laundering and Terrorism Financing), and the National Anti-Narcotics Agency (regarding information exchange on Prevention and Eradication of the Abuse and Trafficking of Narcotics and Narcotics Precursors). Security alerts are provided by exchange of information between the BI and other supervisors. PSPs are required to submit reports regarding the security alert information to the BI.

Collaboration between the supervisory authorities and national banking associations and/or payments associations for the exchange of information on security incidents is also a common practice in several jurisdictions, such as Italy, Macedonia and Portugal.

Financial sector CERT[17] (CERTFin) in Italy

In December 2016, the Bank of Italy and the Italian Banking Association (ABI) established the Italian financial CERT (CERTFin), a cooperative public-private initiative aimed at increasing the capacity for cyber-risk management from banking and financial operators and the cyber-resilience of the Italian financial system through an operational and strategic support for prevention, preparation and response to cyber-attacks and security incidents. CERTFin cooperates with a large community of public and private

[17] CERT stands for “computer emergency response team”.

entities and acts as a centralised hub of the financial sector in dialogue with other strategic sectors and operators on cybersecurity topics.[18]

Security alert system between supervisors and PSPs

To prevent cybersecurity risks, several supervisory authorities – for example, the auhority of Singapore – are setting up security alert systems. The Central Bank of the Russian Federation reported that in its jurisdiction a security alert system is being tested and will be launched in 2018. From 2018, EU Member States will also have to implement a complex framework on security incidents.

Notice on Technology Risk Management in Singapore

In Singapore, the Technology Risk Management Notice (Notice 644 and PS(O)A NO5) requires banks, operators and settlement institutions of designated payment systems to report relevant incidents.

Each entity shall notify the Monetary Authority of Singapore (MAS) as soon as possible, but no later than within one hour of the discovery of a relevant incident. Furthermore, the "relevant entity shall submit a root cause and impact analysis report to the Authority, within 14 days or such longer period as the Authority may allow following the discovery of the relevant incident. The report shall contain:

(a) an executive summary of the relevant incident;
(b) an analysis of the root cause which triggered the relevant incident;
(c) a description of the impact of the relevant incident on the relevant entity's
    i. compliance with laws and regulations applicable to the relevant entity;
    ii. operations; and
    iii. service to its customers; and
(d) a description of the remedial measures taken to address the root cause and the consequences of the relevant incident."

A new framework on security incidents in EU Member States in 2018

Incident reporting obligation to PSPs

EU Member States shall ensure that PSPs establish a framework with appropriate mitigation measures and control mechanisms to manage the operational and security risks related to the payment services they provide, according to the new Payment Services Directive (PSD2).[19] As part

[18] http://www.certfin.it/index-eng.html

[19] Directive (EU) 2015/2366/EU of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation

of this framework, PSPs shall maintain effective incident management procedures, including those for the detection and classification of major operational and security incidents. PSPs should provide the competent authority with an updated and comprehensive assessment of the operational and security risks, and on the adequacy of the mitigation measures and control mechanisms implemented in response to those risks on an annual basis or at shorter intervals.[20]

Pursuant to PSD2, PSPs should notify the appropriate authority of major operational or security incidents, without undue delay. In turn, the authority shall, without undue delay, provide the relevant details of the incident to the European Banking Authority (EBA) and to the ECB.[21]

Security incidents handling

EU Member States shall adopt a national strategy on the security of network and information systems, designate a competent authority and a point of contact to ensure cross-border cooperation of EU Member States' authorities, and establish a cooperation framework at the national level, in accordance with the Directive on security of network and information systems (NIS Directive).[22,23]

In particular, each EU Member State shall designate one or more Computer Security Incident Response Teams (CSIRTs) for the banking sector. These teams are responsible for handling risks and incidents in accordance with a well-defined process.

The Directive establishes that security and notification requirements should apply to operators of essential services (banking entities are considered operators of essential services) and to digital service providers to promote a culture of risk management and ensure that the most serious incidents are reported.

Cooperation at the national level is also highly promoted. The competent authority, the single point of contact and the CSIRT of the EU Member State cooperate to fulfil the obligations set out in the Directive.

Alternatively to contribute to the development of trust between the EU Member States and to promote swift and effective operational cooperation, a network of the national CSIRTs is

(EU) No 1093/2010, and repealing Directive 2007/64/EC. EU Member States shall adopt and publish the measures necessary to comply with PSD2 by 13 January 2018.

[20] Article 95 of PSD2.

[21] Article 96 of PSD2.

[22] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. EU Member States shall adopt and publish, by 9 May 2018, the laws, regulations and administrative provisions necessary to comply with the NIS Directive.

[23] For the purposes of this Directive "security of network and information systems'" means the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems" (Article 4 (2) of the Directive).

established.[24] The EU may conclude international agreements with third countries or international organisations.[25]

The operators of essential services should take appropriate and proportionate technical and organisational measures to manage the risks posed to the security of network and information systems used. They should likewise notify without undue delay the competent authority or the CSIRT of incidents having a significant impact[26] on the continuity of the essential services provided. This notification shall include information enabling the competent authority or the CSIRT to determine any cross-border impact of the incident.[27]

Notification of a personal data breach

From 25 May 2018, the EU Member States will apply a harmonised framework on the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data, established by the General Data Protection Regulation (GDPR).[28]

The GDPR establishes a notification requirement when a personal data breach occurs. The entity, which determines the purposes and means of the processing of personal data ("controller"), shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority.[29]

[24] Article 12 of the NIS Directive.

[25] Article 13 of the NIS Directive.

[26] In order to determine the significance of the impact of an incident, the following parameters, in particular, shall be taken into account: (a) the number of users affected by the disruption of the essential service; (b) the duration of the incident; (c) the geographical spread with regard to the area affected by the incident.

[27] Article 14 of the NIS Directive.

[28] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[29] Article 33 of the GDPR.

Challenge 3	**Close cooperation between conduct of business supervisors and 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**

Scope

- Building trust in digital transactions is an important factor for the proliferation of digital payments. "Consistent governance and a strong cooperation between stakeholders to deal with the potential security issues"[30] is necessary to achieve confidence.
- A structured and collaborative supervisory approach is relevant when dealing with digital payments. Collaboration should be enhanced not only among financial supervisors but also with non-financial supervisors and other entities, at the domestic and international level.[31]
- Conduct of business supervisors often play a role in setting-up multidisciplinary groups – comprised of prudential supervisors, payment systems overseers and other relevant entities − to discuss security incidents and actions to mitigate related risks.
- The security of digital transactions depends on the establishment of a comprehensive, integrated and expedited system for incident response involving all relevant stakeholders.
- Strong cross-border cooperation among all players is key to mitigating security risks raised by the growth of the cross-border provision of digital payment services, from a financial consumer protection and a systemic risk control perspective, notwithstanding the prevention of money laundering and terrorism financing, and the smooth functioning of payment systems.

[30] EPC, *White Paper Mobile Payments*, 2017.
[31] FinCoNet, *Online and mobile payments: Supervisory challenges to mitigate security risks*, 2016.

Main findings from the questionnaire's responses

Graph 3 Close cooperation between supervisors and other relevant entities[32]

- The existence of multidisciplinary formal groups focused on digital payments and security issues at the national level was reported by several respondents.
- The setting-up of partnerships with other relevant entities at the domestic level focused on security risks is an approach pursued by a substantial number of respondents. Some jurisdictions reported that they are in the process of establishing such partnerships.
- The existence of platforms at the national level in order to exchange information and/or responding to security incidents is a practice also reported by several respondents.
- The majority of jurisdictions indicated that they participated in international fora on security issues to promote the exchange of information and cooperation among supervisors, payment overseers and other relevant entities. Despite the fact that some of the organisations identified are not exclusively focused on security or payments issues, they still include these topics on their agendas.
- A national payments council exists in several jurisdictions and others intend to set up this body in the future.
- The exchange of information regarding security incidents with foreign financial supervisory authorities is a common practice adopted by a great number of jurisdictions.
- In most jurisdictions, supervisory authorities have powers to take administrative action against an authorised PSP where the internal procedures and the financial institution's security system do not comply with the regulations and seems to cause consumers' loss and risks related to cross-border payment services. Other jurisdictions clearly indicated that they pay more attention to the internal procedures and system of financial institutions, rather than to individual and specific cases. They also mentioned that specific cases could be dealt with in court or under civil laws.

[32] See Annex II for the complete set of questions included under this topic in the questionnaire.

- Few respondents indicated that conduct of business supervisors have enforcement powers, and may adopt supervisory procedures against a PSP authorised in another jurisdiction, when a payment service user suffers a loss or is defrauded/scammed through a cross-border payment service provided by that PSP.
- In general, there seem to be multilateral/regional/bilateral arrangements in place which foster cooperation among financial supervisory authorities. These arrangements can facilitate the exchange of information regarding the monitoring and notification among those financial supervisory authorities.[33]

Supervisory practices

Multidisciplinary groups focused on digital payments and security issues

In some jurisdictions, such as Chile, Germany, Mauritius, Peru, Philippines and Russian Federation, digital payments are addressed in from multidisciplinary groups integrating a variety of entities at the national level. In some cases, these kind of groups are led by Governments and, in other cases, by central banks.

National Cyber Security Committee in Mauritius

The National Cyber Security Committee comprises representatives of the Ministry of Information & Communication Technology, Law Enforcement and Regulatory Bodies, National CERT, Critical Sectors, Data Protection Office, vendors and private sector institutions and academia. A decision-making body oversees and monitors the implementation of the National Cyber Security Strategy. This Committee provides a collaborative platform to develop and implement strategies to mitigate growing risks in cyberspace. The role of regulatory bodies, that sit on the Committee, such as the Bank of Mauritius, is to establish, control, inspect and enforce regulations with regard to cyber security; and to encourage organisations to adopt security best practices.[34]

[33] For example, there is a cross-border cooperation mechanism within the EU, so its members, including the financial supervisory authorities, can provide the relevant information to the competent authorities and ask them for some measures when the security incidents are occurred. Please see "Supervisory authorities within the EU boost cross-border collaboration in the supervision of payment institutions from 2018" example.

[34] In the National Cyber Security Strategy 2014-2019 of Republic of Mauritius http://mtci.govmu.org/English/Documents/Final%20National%20Cyber%20Security%20Strategy%20November%202014.pdf

Working group focused on payments in Peru

Under Peru's National Financial Inclusion Strategy, since 2015, the Central Bank has been leading a working group focused on payments.

The working group promotes dialogue between authorities and the private sector to design and implement initiatives to foster digital payments. Current members of the working group include: the Superintendency of Banks, Insurance and Pension Funds (SBS), the Telecommunications Regulator (OSIPTEL), VISA, MasterCard, and representatives of the Central Government and the private sector.

Department of Information and Communications Technology (DICT) in the Philippines

"An innovative, safe and happy nation that thrives through and is enabled by Information and Communications Technology" – DICT vision

REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY

In the Philippines, DICT is the lead agency focused on cyber security issues involving digital payments. The DICT "shall be the primary policy, planning, coordinating, implementing, and administrative entity of the Executive Branch of the government that will plan, develop, and promote the national ICT development agenda"[35].

In some jurisdictions, such as Brazil, Ireland and Portugal, the central banks have set up internal groups integrating different departments in order to have a broader perspective of digital issues, namely cybersecurity risks and digital innovation.

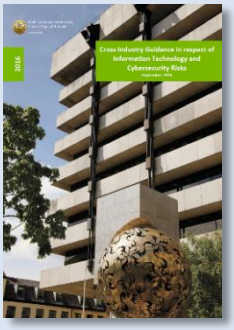
Working group on financial innovation set up by the Central Bank of Brazil

The Central Bank of Brazil (CBB) set up a working group to deal with technological innovation. It aims to advance studies on digital technological innovations regarding the National Financial System and Brazilian Payment System activities, and to assess how those innovations may affect the institutions that comprise those systems, their intermediaries and users, and the CBB itself. This working group has personnel from every area of the CBB, including Supervision, Regulation, IT and Institutional Relations and Citizenship.

[35] http://www.dict.gov.ph/ .

Cross divisional group set up by the Central Bank of Ireland

A cross divisional group (IT and Cyber Risk Strategy Group) was set up to look at common IT and cyber risks across entities supervised by the Central Bank of Ireland, with stakeholders from various divisions such as prudential supervision, conduct of business supervision, and financial stability.



The group focused primarily on cyber risk and published *Cross Industry Guidance in respect of Information Technology and Cybersecurity Risks*,[36] in 2016.

This paper sets out the Central Bank of Ireland's guidance in relation to IT and cyber security governance and risk management by regulated firms in Ireland.

Internal working group on Cybersecurity set up by the Central Bank of Portugal

The Central Bank of Portugal set up an internal and multidisciplinary working group on cybersecurity – composed of the Risk Management Department, the Audit Department, the Financial Stability Department, the Payment Systems Department, the Banking Conduct Supervision Department, the Banking Prudential Supervision Department and the Information Systems and Technology Department –to acquire a global view on the cybersecurity subject to contribute to better and effective coordination internally on this subject, to reflect on a cybersecurity strategy for the Central Bank of Portugal and to define some initiatives to be pursued along with relevant stakeholders.

On 30 July 2017, the Central Bank of Portugal organised a conference on "Cybersecurity in the financial system: risks, cooperation and governance" to discuss (i) the impact of cyber risk in the financial system and business continuity, and (ii) cooperation and governance on cybersecurity in the context of the financial system.[37]

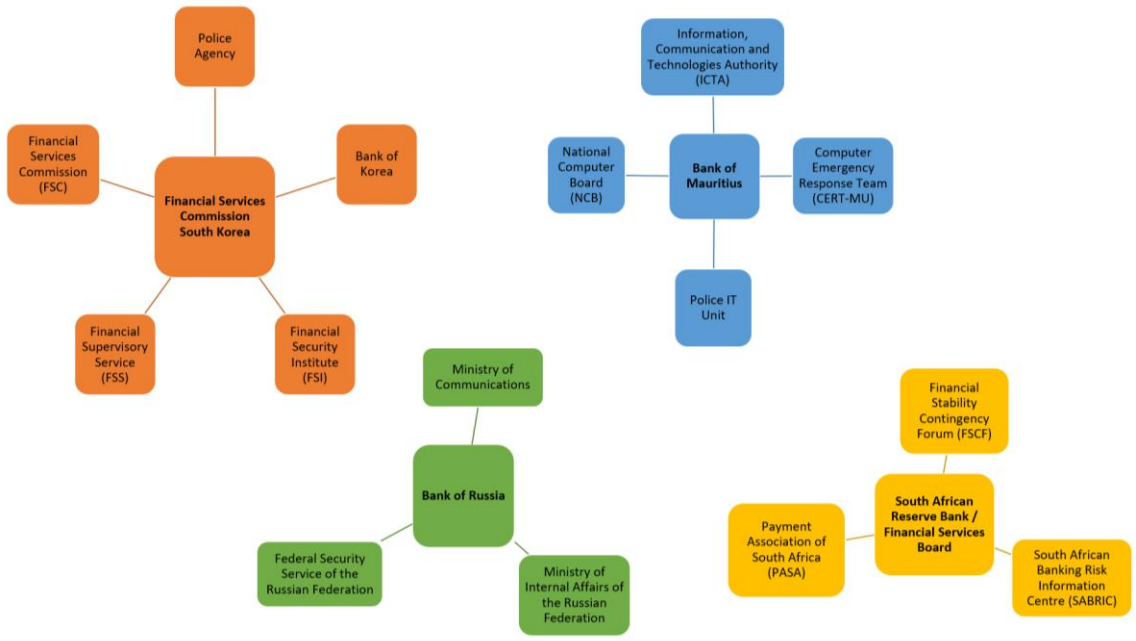
Partnerships focused on security risks

Formal and informal partnerships focused on security risks with different stakeholders are being established at the national level. The partnerships involve a range of entities, from banking associations, police authorities, ministerial departments, national cybersecurity authorities, to payments associations, information and communication authorities, and central banks. Figure 1 provides examples of such partnerships in Mauritius, Russian Federation, South Korea and South Africa.

[36] https://centralbank.ie/docs/default-source/Regulation/how-we-regulate/policy/cross-industry-guidance-information-technology-cybersecurity-risks.pdf?sfvrsn=2

[37] https://www.bportugal.pt/sites/default/files/anexos/documentos-relacionados/intervpub20170630.pdf

Figure 1 Established partnerships at the national level.



Platforms for exchanging information or responding to security incidents among stakeholders are also established by some jurisdictions, as shown in Table 2.

Table 2 Platforms for exchanging information and/or reacting to security incidents

Platforms for exchanging information and/or reacting to security incidents	
Canada	The Association for Commuter Transportation of Canada (ACT Canada) is a national not-for-profit association focused on the evolution of payments and digital identity that brings together issuers, merchants, acquirers, payment networks, regulators and representatives from industry who support them with products and services.[38] FCAC is a member (observer status).
Indonesia	The Task Force on Internet Banking was created by the Bank of Indonesia and is comprised of banks that provide internet and mobile banking services.

[38] http://www.actcda.com/

Japan	Regarding cybersecurity incidents, "Financials ISAC Japan" is an information-sharing body among financial institutions. Information concerning threats, vulnerabilities and responses to incidents is immediately shared via email among members of the "Financials ISAC Japan".
Philippines	Information Security Officers Group (ISOG), Joint Cyber Security Working Group (JCSWG) and Cybersecurity Task Force of the Bankers Association of the Philippines (BAP) serve as *fora* for financial institutions to share or exchange, informally, information related to security incidents.
Singapore	FINTEL is a secure platform established by the Monetary Authority of Singapore (MAS) for sharing cyber intelligence and information pertaining to IT security incidents amongst financial institutions within the country.
United Kingdom	Cyber Security Information Sharing Partnership, sponsored by the National Cyber Security Centre (NCSC), is a joint industry-government initiative. It is the national platform for the exchange of cyber threat information in real time, in a secure, confidential and dynamic environment.[39]

Participation in international organisations

Conduct of business supervisors are regularly participating in international organisations to deepen their knowledge of new security risks and actions to mitigate them, as well as to track global trends in the digital ecosystem. These *fora* are crucial to disseminating best practices. Several international organisations, which have supervisors as members, create in their structure specific work streams to exchange information and cooperate on payments and security issues. In other organisations, regular meetings allow members to discuss payment and security issues. Figure 2 highlights the international organisations identified by respondent jurisdictions.

[39] https://www.ncsc.gov.uk/cisp

Figure 2. Illustration of international fora where payments or security issues are discussed

National Payments Council

A National Payments Council is established in several jurisdictions to provide a forum for supply-side and demand-side stakeholders to discuss issues related to payment services, such as payment solutions, promotion of payment systems interoperability, and definition and implementation of a national payments strategy. It is possible to identify different compositions/structures and responsibilities (mandates) assigned to national payments councils across respondent jurisdictions. Some jurisdictions are working on the establishment of a payments council, namely Lithuania and Mauritius, and the EC indicated that an existing EU Forum is in the process of being transformed into a forum of national payments councils.

National payments councils around the world

Estonian Payment Forum

The Estonian Payment Forum is led by Eesti Pank (Bank of Estonia), working closely with the Ministry of Finance and the Estonian Banking Association. The members of the forum are Estonian credit institutions, users of payment systems, stakeholder representatives including public sector and business and trade organisations, and infrastructure companies. The forum meets twice a year.

Some of the main roles of the Estonian Payment Forum are to develop the payments market and improve payment services; provide consultation on changes to rules affecting the payments market; raise awareness of payment arrangements, payment services and the payments market; involve interested institutions and businesses in discussions on the problems of the payments market and

help agree common positions; exchange information and experiences to give a better understanding of the payments market; and make recommendations for how payment services could be improved.[40]

Observatory for the Security of Payment Means (OSPM) in France

Created by the Law of 9 December 2016 on transparency, the OSMP is a forum for fostering the exchange of information and consultation among all the parties concerned with the smooth functioning of payment means and the fight against fraud.

It is tasked with monitoring the security measures adopted by payment industry participants and their customers, establishing aggregate fraud statistics and maintaining a technology watch in the area of payment means. Among other things, the Observatory monitors the data protection measures taken by the issuers and the traders, the compilation of fraud statistics and the technological watch in regard to payment cards with the object of providing a means of combating technical attacks on the security of payment cards.

The OSMP is chaired by the Governor of the Central Bank of France and comprises two members of parliament, representatives of the government and of card issuers, users (merchants, businesses and consumers), and several individuals chosen for their expertise.[41]

***Forum Zahlungsverkehr* (Payments Forum) in Germany**

The *Bundesbank* set up the Payments Forum – a platform that facilitates dialogue among providers and users of payment services on impending innovations, the design of SEPA 2.0 for digital payment methods and potential areas of conflict. Besides facilitating interaction, the Payments Forum enables participants to explore high-level solutions to a wide range of challenges. The Payments Forum is led by the Board member of *Bundesbank* responsible for payments. Other members are the top-level representatives of both payment providers and payment users. The forum is also attended by representatives from the Federal Ministry of Finance, the Federal Ministry of Justice and Consumer Protection, the Federal Competition Office (Bundeskartellamt) and BaFin.[42]

Indonesia Payment System Forum (FSPI)

Established in 2015 as a cross-institutional forum, the FSPI is evolving into a *forum* for effective coordination, communication, and harmony among the Bank of Indonesia, the Financial Services Authority, the Ministry of Finance, the Ministry of Trade, and the Ministry of Communication and Information in supporting the implementation and development of the Payment System in Indonesia.

[40] http://www.eestipank.ee/en/payments/estonian-payment-forum

[41] https://www.banque-france.fr/en/financial-stability/observatory-security-payment-means

[42] https://www.bundesbank.de/Redaktion/EN/Standardartikel/Tasks/Payment_systems/sepa_payments_forum.html?nsc=true&https=1

Irish Payments Council (IPC)

The IPC is the strategic, representative, administrative and payments system integrity body for the payments industry in Ireland. The IPC is an industry representative body only and has three core objectives: (i) develop and lead a strategic vision for payments; (ii) ensure payment systems and schemes are open, accountable and transparent, and (iii) ensure the integrity and effectiveness of payment systems and payment schemes.

IPC's role is also to provide administrative and operational support to any payment system or payment scheme or the participants therein.[43]

Italian Payments Committee (IPC)

In 2015, the Bank of Italy established the IPC, a cooperative forum with the main objective of fostering the development of a secure, innovative and competitive market for private and public payments in Italy. It responds to global challenges and aims to meet the needs of users (enterprises, households and public administrations). This committee also provides a permanent forum for discussing key issues pertaining to the payment industry, including the risks related to innovative payment services.

The IPC is chaired by the Bank of Italy. Its members are representatives of the supply and demand side of the market (representatives of the banking community, payment institutions, retailers and consumers), PSPs (banks, post offices, and payment institutions), technical service providers and the public administration.[44]

Payments Council on Financial Innovation in Japan

In Japan, the FSA established a "Payments Council on Financial Innovation." The Council aims "to set up a framework in which members from the financial sector, industry, consumer and government work together to follow up the progress on the action plan approved by the Working Group on Payments and Transaction Banking of the Financial System Council, and to deliver payment system reform and payment service innovation continuously."[45]

Payment Systems Forum in Portugal

The Payment Systems Forum's goal is to promote dialogue among the main national stakeholders involved in retail payments. It is an advisory structure of the Central Bank of Portugal, comprising representatives of the national banking community and of the main users of retail payment instruments, such as consumer associations, general government bodies and the corporate sector.[46]

[43] https://www.bpfi.ie/about-bpfi/about-us/payments/

[44] https://www.bancaditalia.it/compiti/sispaga-mercati/comitato-pagamenti-italia/index.html?com.dotmarketing.htmlpage.language=1

[45] http://www.fsa.go.jp/en/news/2016/20160606-1.html

[46] https://www.bportugal.pt/en/page/payment-systems-forum

Comité Nacional de Pagos in Spain

In Spain, the Comité National de Pagos is chaired by the Bank of Spain and has representatives from both the supply (namely, banking associations, representatives for payments industry and card schemes) and demand sides (consumers, small and medium enterprises, IT sector, public administration representatives), as well as representatives from the public sector. Its main purpose is to foster the development of payment services, instruments and infrastructures that contribute to the general economy's competitiveness and efficiency.

Singapore Payments Council

The Monetary Authority of Singapore (MAS) announced on 2 August 2017 the establishment of a Payments Council, comprising 20 leaders from banks, PSPs, businesses and trade associations. The Payments Council will formally bring together both the providers and users of payment services; and will encourage collaboration within the payments industry, promote interoperability among e-payments solutions, and develop strategies to drive the pervasive adoption of e-payments, and advise and make recommendations to MAS on payments related policies.[47]

Information exchange with foreign financial supervisors

The exchange of information regarding security incidents with foreign financial supervisory authorities is done by financial supervisory authorities with the use of different kinds of platforms and/or collaborative procedures – for instance based on a Memorandum of Understanding (MoU) between jurisdictions, such as Indonesia and the Philippines, and/or cooperative oversight arrangements.

Supervision of cross-border payment services

Several multilateral/regional/bilateral arrangements are in place to foster cooperation among financial supervisory authorities. These arrangements can facilitate the exchange of information regarding the monitoring and notification of security incidents among financial supervisory authorities. With the entry into force of PSD2, EU Member States will have to implement a more effective cross-border cooperation mechanism. However, it seems that more attention is given to PSPs' internal procedures and systems, rather than to individuals and users being defrauded.

[47] http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-Establishes-Payments-Council.aspx

Supervisory authorities within the EU boost cross-border collaboration in the supervision of payment institutions from 2018

Competent authorities of the home Member State shall cooperate with the competent authorities of the host Member State of the agent or branch of a payment institution located in the territory of another Member State,[48] in relation to:

On-site inspections

- The competent authorities of the home Member State notify the competent authorities of the host Member State where they intend to carry out an on-site inspection in the territory of the latter.
- The competent authorities of the home Member State may delegate to the competent authorities of the host Member State the task of carrying out on-site inspections.

Report on the activity

- The competent authorities of the host Member State may require payment institutions having agents or branches within their territories to report periodically to them on the activities carried out in their territories.
- Such reports are required for information or statistical purposes and to monitor compliance with the provisions of national law on transparency of conditions and information requirements, and rights and obligations in relation to the provision and use of payment services.

Information on infringements or suspected infringements

- The competent authorities shall provide each other with all essential and/or relevant information in the case of infringements or suspected infringements by an agent or a branch, and in the context of the exercise of the freedom to provide services.

Central contact point

- Member States may require payment institutions operating on their territory through agents under the right of establishment, the head office of which is situated in another Member State, to appoint a central contact point in their territory to ensure adequate communication and information reporting.

Framework for cooperation

- EBA is developing draft regulatory technical standards (RTS) specifying the framework for cooperation, and for the exchange of information, between the competent authorities of the home and host Member States.

[48] Article 29 of PSD2.

- The RTS shall specify the method, means and details of cooperation in the supervision of payment institutions operating on a cross-border basis and, in particular, the scope and treatment of information to be exchanged, to ensure consistent and efficient supervision of payment institutions exercising cross-border provision of payment services.

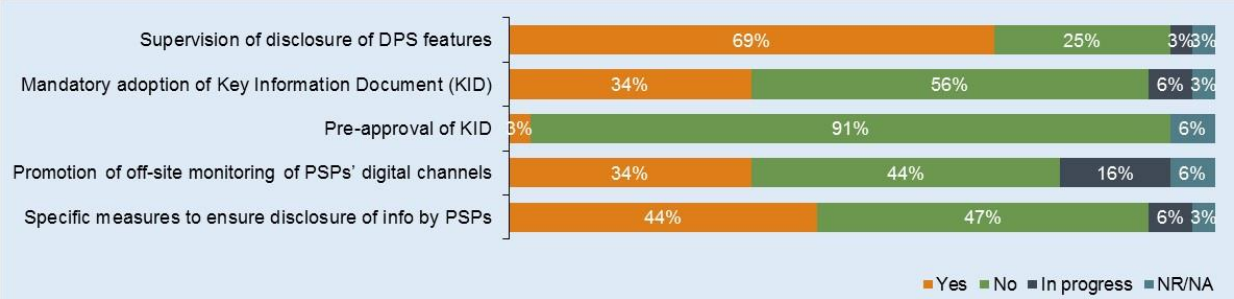
Challenge 4	**Close supervision of PSPs to ensure the implementation and adoption of rules leading to the disclosure of the features of each payment service, their specific risks and the security procedures available to the user in relation to each payment transaction**

Scope

- The growth of supply of and demand for digital payment services poses quite significant regulatory and supervisory challenges, in particular in regard to achieving high standards of transparency and disclosure of information on digital financial markets.
- Ensuring disclosure of clear, transparent, accurate and complete information on digital payments is essential to enable consumers to make safe and enlightened decisions, and to mitigate security risks posed by online and mobile payments, pre-conditions to reinforce consumer confidence in this market.
- To meet these objectives, conduct of business supervisors may oversee PSPs' disclosure of information on the specific features and risks of each payment service, and on security procedures they make available to users.
- Conduct of business supervisors may also use a variety of oversight tools, including off-site monitoring of PSPs' digital channels or the pre-approval of a Key Information Document (KID) on each payment service, to assess compliance with mandatory requirements on the disclosure of risks and precautionary procedures.
- In order to seek PSPs compliance with the regulatory framework, conduct of business supervisors' mandates may encompass enforcement powers. In case of infringement, this would enable supervisory authorities may issue specific orders or, according to the gravity of the irregularity, impose penalties and sanctions.

Main findings from the questionnaire's responses

Graph 4 Close supervision of PSPs' disclosure of information[49]



- Disclosure of digital payment services' features is supervised by the majority of the respondents, to the extent that the payment service is provided by a PSP within the scope of its supervisory perimeter. In most cases, non-financial providers are excluded since they fall out of the scope of the supervisory perimeter.
- Respondents pointed out that there is not yet a specific regulatory framework applicable to disclosure of information on digital payment services. General rules apply to all products and at all levels of the customer's involvement with banking retail products, irrespective of the delivery channel or the technological platform used to perform the transaction.
- Most of the respondents reported that PSPs are not required to adopt a KID and, even within the jurisdictions where the adoption of a KID is mandatory, such a document is not subject to the supervisory authority's pre-approval.
- Although off-site monitoring of PSPs' digital channels to access their compliance with mandatory requirements on the disclosure of security risks and precautionary measures is not being promoted in most jurisdictions on a systematic basis, several of respondents reported that their jurisdictions were already developing these kinds of supervisory initiatives on an *ad hoc* basis.
- Specific measures to ensure disclosure of information to payment service users are being developed by several conduct of business supervisors, including the publication of codes of conduct and the implementation of guidelines addressing particular concerns often inspired by international standards.

Supervisory practices

Disclosure of digital payment services features

Specific supervisory measures addressing disclosure of information on the digital environment are already being developed in some jurisdictions. The Dutch AFM uses an incident-based and thematic

[49] See Annex II for the complete set of questions included under this topic in the questionnaire.

approach, using signals from consumers and market players to develop and implement a supervisory strategy on disclosure of information on digital payment services. The AFM assesses financial information leaflets after they have been published and once the firm starts selling the financial product in question. However, some firms proactively ask the AFM to check the text of their leaflets before they start selling the product.

Adoption and pre-approval of the Key Information Document

In a large number of jurisdictions, the adoption of a KID concerning a specific digital payment service is not mandatory, but in some of them the respective supervisory authority sets specific information requirements for regulated PSPs. In others jurisdictions such as Canada, Indonesia, Mauritius and Portugal, PSPs are already obligated to adopt such a document.

FCAC Information summary box examples in Canada[50]

FCAC reported that federal regulations applicable to federally regulated entities prescribe specific requirements on the content and timing of disclosure for different financial products and services (including digital payment services). Among the requirements is the provision of information summary boxes for customers. These requirements are applicable when a payment service is provided by an federally regulated financial entity (FRFE) - that is, a bank - or an affiliate of such an entity, and is specific to credit cards.

Standardised information sheet for current accounts in Portugal

In Portugal, since 2009, a Notice issued by the Central Bank of Portugal under its conduct of business mandate obligates PSPs to provide consumers with a standardised information sheet prior to the opening of a bank account, including its main features, irrespective of the channel used.

Even in jurisdictions where the adoption of a KID is mandatory, the document is not subject to pre-approval by the conduct of business supervisor.

However, the Central Bank of the Republic of the Philippines reported that it is developing a type of pre-approval mechanism where the contractual terms and user agreements for certain digital payment services or channels would be reviewed or evaluated as part of the financial institution's application to provide that service.

[50] https://www.canada.ca/en/financial-consumer-agency/services/industry/commissioner-guidance/guidance-4.html

Other supervisory authorities, such as the Financial Consumer Agency of Canada, stated that while there is no legal requirement to pre-approve disclosure documents, regulated entities may proactively reach out to the supervisor to ensure the material is compliant with the regulations.

Off-site monitoring of PSP's digital channels

Off-site monitoring of PSP's websites, home banking, APPs and other digital channels to assess their compliance with mandatory requirements on the disclosure of precautionary measures is being promoted or is about to be implemented within several jurisdictions, such as Armenia, Germany and Portugal.

Off-site monitoring as a supervisory tool in Armenia, Germany and Portugal

The Central Bank of Armenia is conducting off-site monitoring of PSPs' websites and other delivery channels to check compliance with the applicable regulations on a quarterly basis.

In Germany, concerning off-site monitoring of digital channels performing regular penetration tests for the most critical systems is already regarded as standard practice that has to be accomplished by banks. Under the upcoming PSD2, as pointed out by BaFin, this requirement will be strengthened, especially in the context of digital payments.

The Conduct of Business Supervison Department at the Central Bank of Portugal is developing a supervisory strategy regarding innovative financial services, in particular, through APPs. Applying a risk-weighted approach, the Central Bank of Portugal is asking supervised institutions to complete a specific questionnaire to collect information on the main features of the financial products and services provided through APPs, to evaluate compliance with disclosure requirements and to assess the security procedures implemented.

In other jurisdictions, such as Canada and Estonia, where a systematic off-site monitoring strategy is not in place, conduct of business supervisors are developing similar supervisory initiatives on an ad hoc basis, relying on complaints handling or other sources of information.

Specific measures to ensure the disclosure of information

EU Member States reported having implemented the EBA Guidelines on the security of internet payments [51], which establish a set of minimum requirements in the field of the security of internet payments, including specific disclosure on security risks and information to be mandatorily provided to users. These jurisdictions also highlighted the transposition of the PSD2, given that it implies quite significant changes to the current supervisory and regulatory landscape. In this context, EU Member States will be asked to implement the *Regulatory Technical Standards on strong customer*

[51] https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29_Rev1

authentication and secure communication (RTS).[52] The final draft was published in 2017 by the EBA and submitted to the EC.[53] The proposed RTS seek to achieve the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the EU. With regard to the supervision and oversight of digital payment services, the RTS enhance the need for PSPs to ensure transparency and disclosure of the security procedures available to the user in relation to each payment transaction.

Innovative initiatives to ensure disclosure of information in the digital ecosystem in Mauritius, Peru and South Africa

In Mauritius, according to the *2015 Guideline on Mobile Banking and Mobile Payment System*, [54] PSPs should walk potential users through the entire process to educate them about the possibilities of misuse or failure of technology, and to remove psychological obstacles to trying the technology and improve user-friendliness. Regarding the promotion of preventive safety behaviours, the *Guideline on Mobile Banking and Mobile Payment Systems* requires PSPs to run information campaigns and maintain ongoing helpdesks for customers to cover at least the following topics: (i) advise customers on the benefits of having different Personal Identifications Numbers (PINs) for different online services; (ii) provide instructions to customers on how to configure their mobile devices to access mobile and payment applications; (iii) advise customers to take security precautions in using mobile banking and payment services; (iv) advise customers on dispute handling, reporting procedures and the expected time for resolution; and (v) avoid the use of complex, legal and technical jargon in their communications with customers. Under the *2001 Guideline on Internet Banking*,[55] each institution offering banking products and services over the internet should have a 'Client Charter on Internet Banking' prominently displayed on its website. This Charter should, at minimum, state each institution's commitment to ensuring safe operations, privacy of customer information, reliable and quality services, transparency of products and services, and prompt response to enquiries and complaints.

In Peru, within the framework of the Financial Inclusion National Strategy, the supervisory authority is promoting an assessment of transparency and disclosure rules on retail payments and e-money transactions to regulate the use of nomenclature in the definition of products for market.

The Payments Association of South Africa (PASA) seeks to communicate the functionality and features of particular products used by the general public. Examples include the misuse and abuse of the early debit order system, authenticated collections and biometrics.

[52] https://www.eba.europa.eu/documents/10180/1761863/Final+draft+RTS+on+SCA+and+CSC+under+PSD2+%28EBA-RTS-2017-02%29.pdf

[53] The draft Guidelines are subject to the principle of proportionality, which means that all PSPs are required to be compliant with all Guidelines, but the precise steps that they are required to take to be compliant may differ between PSPs, depending on their size, business model and complexity of their activities.

[54] https://www.bom.mu/sites/default/files/Guideline_Mobile_Banking_Mobile_PaymentSystem2.pdf

[55] https://www.bom.mu/sites/default/files/Guideline_on_internet_banking.pdf

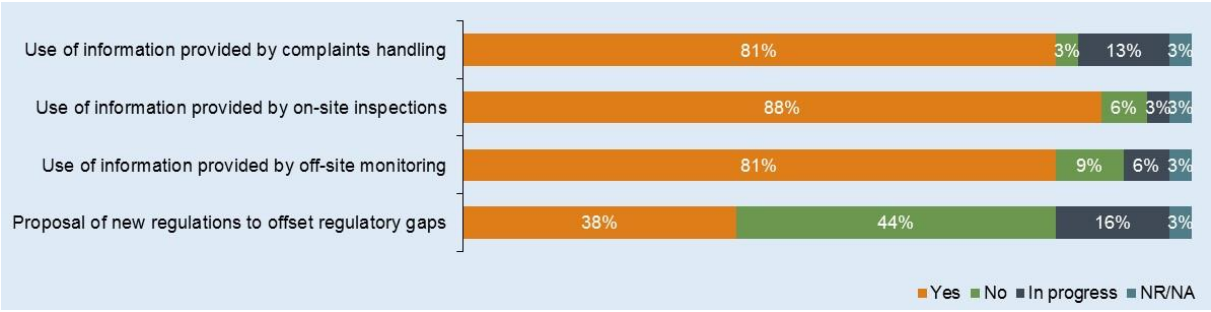
Challenge 5	Ongoing assessment of security risks through the use of a variety of supervisory tools, particularly with respect to the management of complaints, to identify the most common and the new security risks and their importance for consumer protection, allowing supervisors to promote targeted actions, which could include the identification of regulatory gaps

Scope

- In tandem with close cooperation between prudential supervisors and payments overseers, conduct of business supervisors may rely on different supervisory tools to assess security risks. The efficiency of traditional supervisory tools may be questioned as the financial consumer protection framework is being challenged by the complexity of the digital payments market.
- Within the scope of conduct of business supervision, complaints handling will keep playing a key role, allowing supervisory authorities to assess PSPs' compliance with the regulatory framework, and to identify the most significant security incidents and the PSPs involved. Other oversight tools, including on-site inspections and off-site monitoring, may need to be reviewed to adopt new methodologies to enhance monitoring and oversight of PSPs.
- Analysis of data collected by means of different supervisory tools represents a valuable resource when tracking new business trends and PSPs' current practices, and when identifying and proposing regulations to address regulatory gaps,

Main findings from the questionnaire's responses

Graph 5 Ongoing assessment of security risks through supervisory tools[56]



[56] See Annex II for the complete set of questions included under this topic in the questionnaire.

- Collected data from complaints handling is being used by the majority of conduct of business supervisors to identify most significant security incidents and the PSPs involved in these incidents. The supervisors use this knowledge to prevent and mitigate security risks.
- Many respondents use information garnered from on-site inspections to identify security risks and plan risk mitigation initiatives, whether as part of a thematic programme of inspections or as reactive inspections to oversee more in-depth issues identified in the process of complaints handling.
- Information gathered from off-site monitoring was reported to be used by the majority of conduct of business supervisors to identify security risks and to plan risk mitigation initiatives. This finding underscores the importance of cooperation and exchange of information between prudential and conduct of business supervisors.
- New regulations to offset regulatory gaps identified by various supervisory tools were reported to have been recently proposed by several jurisdictions. The majority of these new regulations concern fraud prevention.

Supervisory practices

Complaints handling to identify security risks and plan risk mitigation initiatives

Some conduct of business supervisors, such as those from France and Spain, reported using information from complaints to identify security risks. In the case of France, data from complaints are used on a risk-weighted basis and, when appropriate, are shared with the Central Bank of France. However, this country does not yet use information from complaints to develop risk mitigation initiatives.

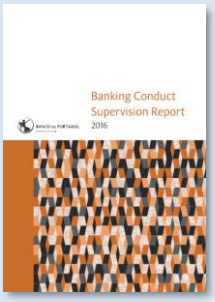
Cooperation with prudential supervisors or payment overseers regarding security issues was also highlighted by other respondents, such as the Dutch AFM, which shares complaints data on security risks with the Dutch Central Bank, the entity responsible for monitoring security incidents and procedures.

The majority of respondents are using collected data to plan risk mitigation initiatives. The Banking Conduct Supervision Department of the Central Bank of Portugal uses the information provided by complaints handling to schedule on-site inspections, to implement risk mitigation measures, to plan awareness campaigns and education initiatives, and to conduct closer monitoring of specific supervised institutions' security procedures. In the same way, in Germany, if unusual clusters are detected, BaFin may conduct specific off- and on-site inspections or send questionnaires to PSPs to better assess the first findings.

Conduct of business supervision reports in Portugal and Spain

Within a framework of transparency and accountability, several supervisors, such as the Central Bank of Portugal and the Central Bank of Spain, publish reports on their conduct of business activities.

In Portugal, the Banking Conduct Supervision Reports have presented since 2008 on a yearly and half-yearly basis the Central Bank's activities under its financial consumer protection strategy, in particular, when monitoring financial institutions' compliance with the applicable regulatory framework. In this regard, complaints-handling data such as the level of complaints per credit institution (in relative terms, taking into account the size of the business) and the most claimed matters, as well as data on the systematic monitoring and inspections, are published. [57]



Similarly, Spain issues an annual complaints report of the Market Conduct Department of the Central Bank of Spain that discloses data on complaints handling and criteria used by Banco de España for solving complaints presented by customers against financial entities. Moreover, Banco de España publishes the Banking Supervision Report, that encompasses all supervision activities performed during the year, including market conduct supervision activity. [58]

Complaints handling is reinforced by new regulations on payment services in EU

From 2018, competent national authorities of EU Member States will have to comply with the EBA *Guidelines on procedures for complaints of alleged infringements of the PSD2*,[59] following obligations imposed by PSD2 on complaints handling.

These guidelines, published on 3 October 2017, address complaints procedures to be adopted by the competent authorities designated by each Member State to ensure and monitor effective compliance with the PSD2. In particular, the guidelines require competent authorities to make an aggregate analysis of the complaints received, to document their internal complaints procedures and to make public available information related to their procedures for complaints of alleged infringements of PSD2.

[57] http://clientebancario.bportugal.pt/pt-PT/Publicacoes/RSC/Biblioteca%20de%20Tumbnails/Banking%20Conduct%20Supervision%20Report%20(2016).pdf (executive summary of the report is available in English).

[58] https://www.bde.es/f/webbde/Secciones/Publicaciones/PublicacionesAnuales/MemoriaServicioReclamaciones/16/Ficheros/MSR2016_Documento_completo.pdf (information only available in Spanish).

[59] https://www.eba.europa.eu/documents/10180/1989045/Final+Guidelines+on+complaint+procedures+under+PSD2+%28EBA-GL-2017-13%29.pdf

Information provided by on-site inspections and off-site monitoring

As part of its mandate, the Financial Consumer Agency of Canada monitors and evaluates trends and emerging issues that may have an impact on consumers of financial products and services. Various tools and data can be used, including complaints data, internal assessments, interviews, public reports, etc. One example is research published in 2013 and 2015 on mobile payments and consumer protection.[60]

The AMF of Quebec points out that results of on/off-site inspections are continuously reviewed. Any risk identified, including security risk, is quantified and risk mitigation initiatives are considered and planned if needed.

In the United Kingdom, inspections are not routinely conducted on all firms but may be used as a supervisory tool to support thematic (i.e. multi-firm) work or firm-specific investigations.

In South Africa, the Bank Supervision Department at the Reserve Bank, under its risk-based approach, makes use of information obtained from regulatory engagements, such as on-site inspections, to plan appropriate actions.

New regulations to offset regulatory gaps

Several jurisdictions reported having recently proposed new regulations to offset regulatory gaps identified with supervisory tools, as in Table 3.

Table 3. New regulations to offset regulatory gaps identified with supervisory tools

New regulations to offset regulatory gaps identified through supervisory tools	
Canada	The federal government is currently developing an oversight framework for retail payments to promote a well-functioning payments system that fosters innovation and better protects consumers. This work is being led by the Department of Finance and a consultation paper will be published in 2017. Based on the results of the consultations, the Government will propose legislation to implement the oversight framework. This initiative was announced in the last federal budget under the theme "*Supporting Innovation in Financial Services*".[61] The AMF is planning the publication of an Information and Communication Technology Risk Management Guideline for financial institutions to ensure the development of a holistic view of all ITC risks (and their management) within organisations.

[60] https://www.canada.ca/en/financial-consumer-agency/programs/research.html
[61] http://www.budget.gc.ca/2017/docs/plan/chap-01-en.html#Toc477707370"

EU Member States EU Commission	PSD2 regulates new payment services widening its scope to other PSPs. It comprises the payment initiation service and the account information service. 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 information on one or more payment accounts held by the payment service user with either another PSP or with more than one PSP.
South Africa	The National Payment System Act review currently underway is the result of developments and new entrants and services in the NPS. The emergence of new models, stakeholders and services illustrated gaps in the current regulatory framework necessitating the review. The Bank Supervision Department at the Reserve Bank (BSD) recently issued a guidance note to the South African banking industry stating that the guidance from the Committee on Payments and Market Infrastructures (CPMI) and from the Board of the International Organisation of Securities Commissions on cyber resilience for financial market infrastructures is applicable to banks as well. BSD therefore expects banks to adhere to the guidance in principle and in their individual contexts. Order payment streams have been initiated through issuance of Terms of Reference calling for authentication of early debit orders by the National Payment System Department. The review could enable PASA to regulate and supervise PSPs and users.
Indonesia	The Central Bank of Indonesia issued a regulation on Payment Transaction Processing in 2016, mainly as a response to the rapid change of the payment system industry with respect to e-commerce development and the rise of the FinTech industry. By issuing this regulation, the Central Bank of Indonesia creates a level playing field for all PSPs, by regulating PSPs which were not yet regulated.
Mauritius	National Payment System Legislation will be enacted shortly. This legislation will provide more comprehensive security requirements. The Guideline on Mobile Banking and Mobile Payment Systems is also being reviewed. It will lay more emphasis on security aspects of digital transactions and broaden the scope of application.
Philippines	The Central Bank of the Republic of the Philippines has recently adopted several regulations to combat certain threats/vulnerabilities, which were identified with supervisory tools, including (i) multi-factor authentication requirement – to address “card-not-present fraud”; (ii) management of ransomware and other malware attacks – to address recent attacks (e.g. wannacry) globally; (iii) social media risk management, to manage risks associated with social media platforms; and (iv) fraudulent email and websites, to guide BSFIs in preventing, detecting, responding to and recovering from phishing and pharming attacks.

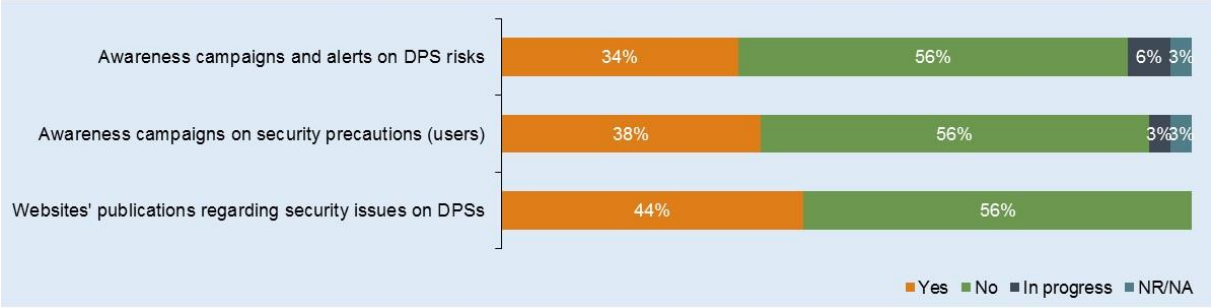
Challenge 6	Promotion of awareness campaigns on risks raised by digital payments, specifically regarding emerging security risks or major security incidents

Scope

- Compliance with regulatory initiatives that assign the responsibility to PSPs to cultivate a culture of informed decision-making and security procedures among their clients may be steered by conduct of business supervisors.
- Supervisors may also acknowledge the importance of campaigns to raise awareness of the risks of digital payments and the responsibility of users to comply with security procedures, promoting balance between convenience and security.
- PSPs shall implement robust systems to prevent security incidents. They shall also have an efficient alert system to warn consumers, when deemed necessary. Supervisors may contribute to the dissemination of these alerts and the respective safeguard measures. Regular publication of information on features and risks regarding digital payment services through booklets, flyers and websites is considered an effective supervisory approach.

Main findings from the questionnaire's responses

Graph 6 Promotion of awareness campaigns on security risks[62]



- Awareness campaigns and alerts focused on the risks of digital payment services and precautionary procedures that users should adopt to prevent security incidents are currently being run by a minority of respondents, although others intend to begin using these measures in the near future.

[62] See Annex II for the complete set of questions included under this topic in the questionnaire.

- Contents regarding security issues related to digital payment services are being released by several conduct of business supervisors on their websites. In some jurisdictions, financial supervisors and other national bodies are setting up partnerships to increase consumer awareness, releasing information on security precautions related to digital payments on a shared website.

Supervisory practices

Awareness campaigns on the risks of digital payments services

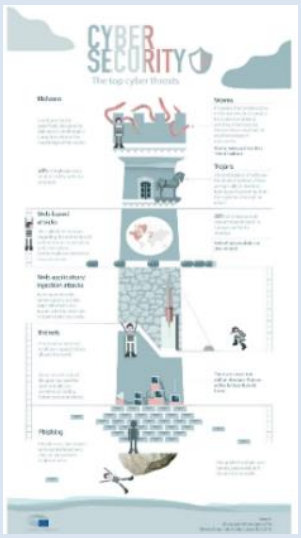
Awareness campaigns and alerts are being conducted through different kinds of initiatives, such as seminars, conferences, electronic media, leaflets, banners, books, and stickers. For instance, in Indonesia, awareness campaigns and alerts are mostly conducted through seminars. In the Philippines, the Financial Consumer Protection Department of the Central Bank regularly holds public *symposia* targeting various stakeholders, including academia and consumers, to promote security consciousness regarding digital payment services. In Portugal, awareness campaigns on security issues related to digital payments are being carried out through the *Portal do Cliente Bancário* (Bank Customer Website created by the Portuguese Central Bank). Social media is used in Canada, Chile, and Singapore to increase consumer awareness of risks raised by digital payments.

The Central Bank of Portugal runs awareness campaigns focused on the digital ecosystem on its Bank Customer Website (*Portal do Cliente Bancário)*

"Protect yourself from online fraud" [63] is an awareness campaign on prevention of online fraud that includes a brief description of fraudulent methods like phishing, pharming and spyware, and a set of security precautions that payment service users should follow to prevent security risks.

Portal do Cliente Bancário also identifies the major security risks raised by digital payments, as well as a set of security precautions to mitigate online fraud. The information provided is updated in keeping with the rapid development of financial innovation.

[63] http://clientebancario.bportugal.pt/pt-PT/Noticias/Paginas/SegurancaOnline.aspx



EU Parliament released an infographic on security risks

The EU Parliament alerted consumers on the most common security incidents in the digital ecosystem.

"Europeans are highly concerned about cyber security: 89% of all internet users avoid disclosing personal information online, while 85% agree that the risk of becoming a victim of cybercrime is increasing. Every day more than 150,000 viruses and other malicious codes circulate." [64]

Awareness campaigns on security precautions

Most of the awareness campaigns run by conduct of business supervisors – e.g. in Brazil, Chile, France, Japan, and the Russian Federation – aim to promote precautionary attitudes among those using payment cards to make digital payments.

Awareness campaigns regarding card payments through digital channels in Brazil, Chile, France, Japan and the Russian Federation

In Brazil, the *Caderno de Educação Financeira – Gestão de Finanças Pessoais* (Guidance on Financial Education – Personal Finance Management) includes self-protection measures recommended for consumers to avoid fraud when using payment cards to make digital payments. Messages include the following: don't lend your card; keep your card in a safe place; keep your PIN absolutely private; install antivirus and firewall in your computer before using internet banking; avoid using public computers and networks for internet banking.[65]

In Chile, the Superintendency of Banks and Financial Institutions has initiated general consumer awareness campaigns regarding the importance of protecting your bank pin code ("cuida tu clave") and other sensitive information.

[64] http://www.europarl.europa.eu/news/en/headlines/security/20160701STO34371/cyber-security-new-rules-to-protect-europe-s-infrastructure

[65] https://www.bcb.gov.br/pre/pef/port/caderno_cidadania_financeira.pdf (only available in Portuguese)

In France, a website dedicated to financial literacy mentions some precautionary measures for users of digital payments services, especially when they use their payment card. The French Observatory for the Security of Payment Means' website provides complementary information.

In Japan, to tackle the increasing number of consumer problems related to prepaid cards in recent years, JFSA has taken various measures, including the publication of a guidebook for financial consumer protection, outlining real situations of fraud involving electronic money. The guidebook is available on JFSA's webpage and is also distributed to high schools, universities and local governments to raise awareness.

The Russian Federation has also published on its website a leaflet on security measures applicable to payment cards, including the use of such cards for online services. The leaflet is intended to be a reference for banks to ensure the quality of their awareness programmes.

In some jurisdictions, awareness campaigns and alerts on digital payments focus on a specific target audience. Canada promotes conferences addressing college students and seniors. The Central Bank of Portugal plans to develop specific content and training sessions for young people, focusing on features, advantages, and risks related to digital payments, as well as on security precautions.

To raise awareness of security issues related to digital payments, the Financial Consumer Agency of Canada has published specific materials focusing on mobile payments and digital currencies,[66] and the Autorité des Marchés Financiers' initiatives focus primarily on internet fraud and protection from identity theft. While the Central Bank of Mauritius published material on risks pertaining to some forms of digital payments in 2016, the country is currently preparing a more comprehensive campaign in view of major forthcoming developments on that front. The Mauritius communication campaign will be rolled out in sync with the implementation of certain projects. In the Philippines, the Central Bank regularly issues public advisories on emerging risks related to digital services as a whole. The South African Reserve Bank has conducted campaigns advising citizens to be wise with their money and not to invest in scams, and PASA has issued media statements to inform users and members of the risks and their rights related to electronic payments.

In some jurisdictions, such as the Philippines, awareness campaigns are regularly conducted in coordination with industry associations.

[66] https://www.canada.ca/en/financial-consumer-agency/services/payment.html and https://www.canada.ca/en/financial-consumer-agency/programs/research.html

Content on security issues

In France, Portugal and Spain, security topics related to digital payment services are highlighted in conduct of business supervisors' activity reports.

Conduct of business supervisors update materials regarding innovative payments and their risks. In Mauritius, informative material outlines trends and technological improvements to mitigate risks raised by the digital ecosystem.

In France, financial authorities [67] operate a website to inform the public about financial firms and services. This website provides consumers with information on security precautions when consumers use their payment cards for internet payments. The Observatory for the Security of Payment Means' website also contains general information and recommendations regarding the security of payments. In Indonesia, the Central Bank's website provides information about security precautions for digital payment services.

In Luxembourg, the conduct of business supervisor's website publishes information on *Security for online banking transactions* and links consumers to the Luxembourg Bankers' Association website, which provides a number of recommendations concerning vigilance to optimise the management of online bank accounts. Consumers are also informed about the information provided by BEE SECURE, a website dedicated to internet security issues. [68]

BEE SECURE in Luxembourg

BEE SECURE's website [69] comprises different content and activities for visitors (including videos, self-assessment tests, [70] documental information) to raise consumer awareness of how to protect their security when using new technologies. In particular, BEE SECURE provides consumers with recommendations related to e-banking, relevant warnings, as well as a helpline offering advice and help. There is information specifically targeting youth, adults and parents.

BEE SECURE is a joint initiative of the Ministry of the Economy, the Ministry of Family, Integration and Greater Region and the Ministry of National Education, Childhood and Youth. It is partly funded by the EC and acts as the Luxembourg awareness centre within the European network, Insafe.

In the Philippines, the central bank's website includes Frequently Asked Questions on digital payment systems and other related topics to financial consumers.

[67] Banque de France, the Autorité de Contrôle Prudentiel et de Résolution, and the Autorité des Marchés Financiers.

[68] http://www.cssf.lu/en/consumer/consumer-information/security-for-online-banking-transactions/

[69] https://www.bee-secure.lu/fr

[70] Such as "*Online Password Test: Tester la résistance d'un mot de passe"*, "*BEE PASS+: Testez vos connaissances en matière de e-commerce/e-banking*" and "*BEE PASS special: Qu'est-ce que le cyber-harcèlement et comment réagir*".

In Spain, several awareness notes and remarks have been published on the Bank of Spain's website concerning the risks and procedures regarding digital payments services. The same type of warnings have been published on the *Portal del Cliente Bancario* (Banking Client Portal) of the Bank of Spain.

In Singapore, the MoneySENSE website provides information to consumers to increase their awareness of security precautions.

MoneySENSE in Singapore

In Singapore, the MoneySENSE website[71] publishes security measures to mitigate security risks.

Making SENSE of Internet Banking Security is an example of a consumer alert on internet banking published in MoneySENSE.[72]

MoneySENSE is the national financial education programme in Singapore. The programme aims to enable consumers to become more self-reliant in their financial affairs.[73]

In the United Kingdom, the Financial Conduct Authority's website has information available on banking and online account scams. In Germany, BaFin's website provides some general information on alternative payment methods, focusing on associated chances and risks.[74]

In the Russian Federation, all PSPs (money transfer operators) are obligated by law to inform their clients of potential risks associated with using digital payment services (before the distribution of any tech linked to that service).

[71] http://www.moneysense.gov.sg

[72] http://www.moneysense.gov.sg/Understanding-Financial-Products/Investments/Consumer-Alerts/Making-SENSE-of-Internet-Banking-Security.aspx

[73] MoneySENSE is spearheaded by the Financial Education Steering Committee (FESC), who is chaired by the Monetary Authority of Singapore (MAS) and comprises representatives from several public sector agencies and government ministries, including the Ministry of Education (MOE), Ministry of Health (MOH), Ministry of Manpower (MOM), Ministry of Social and Family Development (MSF), Central Provident Fund Board (CPFB), National Library Board (NLB) and People's Association (PA). MAS also serves as the secretariat to the FESC. Information available at http://www.moneysense.gov.sg/About-MoneySENSE.aspx.

[74] Alternative payment methods ("*Alternative Bezahlverfahren*") – https://www.bafin.de/dok/8894790. There is also an article in BaFin's news bulletin *BaFinJournal* (August 2015 issue, pages 15 -19) dealing with "Online-Banking: Security aspects from a consumer protection perspective" – https://www.bafin.de/dok/7868854 (only available in German).

Challenge 7	Coordinated approach between conduct of business supervisors and national bodies responsible for financial literacy to promote the use of precautionary procedures by digital customers

Scope

- Digital financial literacy is increasingly at the top of the international agenda[75] and is being globally recognised as essential for the financial empowerment of individuals and the overall stability of the financial system.[76]
- Digital financial literacy initiatives conducted by supervisors in collaboration with financial literacy bodies contribute to a more secure environment for digital payments. These collaborations promote precautionary attitudes and safety procedures by users, enhancing the impact of supervision-based information.
- Conduct of business supervision may be focused not only on the provision of financial services, but also on the demand side, fostering consumers' financial capability.
- Even when conduct of business supervisors do not have an explicit mandate to promote financial literacy, they may consider developing financial literacy initiatives on their own or in collaboration with other financial literacy bodies to disseminate information on the features and risks of digital payment services and to raise awareness about the adoption of secure procedures by users.
- A digital financial literacy strategy needs to promote not only financial inclusion, but also needs to prevent the ageing population from the risk of becoming financially excluded.

[75] The G20 recognises that "it is crucial to take concrete and significant actions to advance digital financial inclusion under the guidance of the G20 High-Level Principles for Digital Financial Inclusion", which have been prepared by G20-GPFI (available at https://www.gpfi.org/publications/g20-high-level-principles-digital-financial-inclusion).

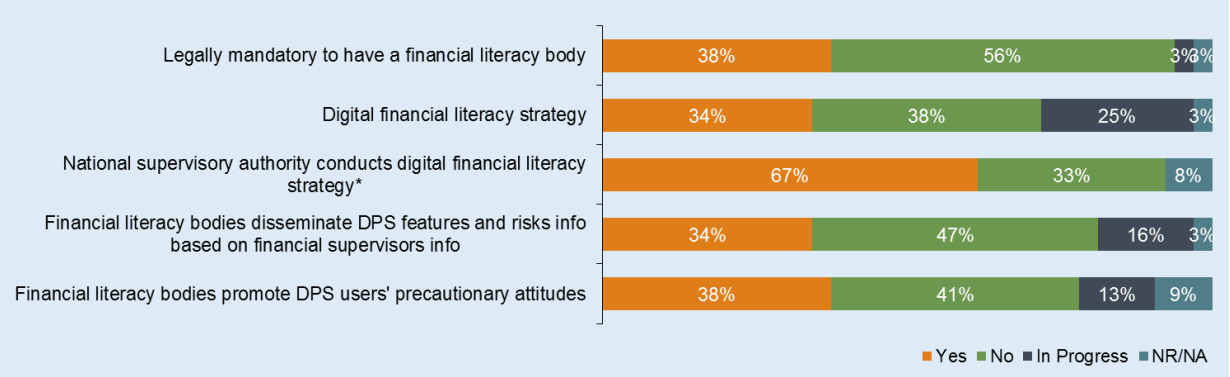
The OECD/INFE *Ensuring financial education and consumer protection for all in the digital age* report "highlights the need to further enhance consumer protection and financial education frameworks to more effectively target digital finance, and identifies financial literacy initiatives and policy options that can help consumers better manage any potential digital risks and benefits. It illustrates the use of digital tools to deliver financial education, while addressing the role of public, private and other relevant stakeholders in this regard" (available at http://www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-Report-Financial-Education-Consumer-Protection-Digital-Age.pdf).

Child & Youth Finance International, sometimes in partnership with national supervisors, is also working in digital financial services. For instance, see the booklet *Staying safe online – youth and digital security* (available at https://finansdanmark.dk/media/14406/staying-safe-online-youth-and-digital-security-2016.pdf). This booklet on digital security is an abridged and international version of the original Danish booklet *Unge og Digital Sikkerhed,* which is used in the Danish Money Week from 2017 and beyond.

[76] OECD/INFE, *Ensuring financial education and consumer protection for all in the digital age*, 2017.

Main findings from the questionnaire's responses

Graph 7 Promotion of digital financial literacy[77]



*Refers to those jurisdictions that have a digital financial literacy strategy.

- Although the majority of respondents recognise the importance of financial literacy, an entity with a legally established financial literacy mandate does not exist in a great number of jurisdictions.
- From the analysis of the responses, the existence of a specific financial literacy strategy targeted at digital financial services was only reported by a few number of respondents. Nonetheless, several respondents have financial literacy programmes that include content on digital financial services.
- Several respondents stated that, where there is a digital financial literacy strategy, the national supervisory authority should be responsible for its implementation. In some cases, the responsibility for financial literacy strategy is shared between the national supervisor and other bodies, such as ministries.
- The financial literacy body (or bodies), in several – albeit, not most – jurisdictions, disseminates information on the features and risks of digital payment services based on information provided by the financial supervisors, such as research and statistics regarding digital payment services and risks.
- According to respondents from several jurisdictions, the financial literacy body (or bodies) should run initiatives and campaigns to promote precautionary attitudes through websites, Facebook, videos or education programmes. However, most respondents do not yet run these kinds of initiatives.

[77] See Annex II for the complete set of questions included under this topic in the questionnaire..

Supervisory practices

Legally mandatory financial literacy body

In Canada, the Financial Consumer Agency of Canada Act gives FCAC a dual mandate: to supervise federally regulated financial entities and to promote financial consumer education and literacy. The AMF of Quebec has a department exclusively dedicated to financial education and reinvests funds from penalties into awareness campaigns, outreach projects and academic research (AMF Quebec Education and Good Governance Fund). In Indonesia, a Presidential Regulation (No. 82/2016) concerning the Financial Inclusive National Strategy establishes a Financial Inclusive National Council, with a working group on Financial Education. In the United Kingdom, the Money Advice Service was set up as an independent body, in April 2010, with responsibility for improving people's money management. In Italy, in 2017, Parliament passed a law that sets up the National Strategy on Financial Education and a National Committee has been created to plan and coordinate financial education activities.

Despite the fact that it is not mandatory to have a financial literacy body, some jurisdictions have already implemented specific programmes that demonstrate a great interest in financial literacy. For instance, in South Africa, PASA runs a Payments Foundational Course to educate participants in the national payment system on all aspects of payments, including digital payments.

Digital financial literacy strategy

The Bank of Indonesia conducts two financial literacy activities – one, focused on electronification and the other on financial inclusion. In other jurisdictions, such as Portugal, there are financial literacy programmes that include contents about digital financial services.

Plan for the Financial Education of the Public in Lithuania

The Bank of Lithuania, in collaboration with the Ministry of Finance, Ministry of Education and Science, State Tax Inspectorate and SoDra aims to improve residents' habits of saving for the future, and to encourage to them to select appropriate financial products and services, and to pay taxes as required. To achieve these goals, in May 2017, the institutions jointly prepared and will implement a Plan for the Financial Education of the Public. The Plan sets out that the Bank of Lithuania will run a consumer financial education campaign encouraging residents to select the right financial products and services for them, and to save for the future. The Ministry of Education and Science will include financial and tax literacy in formal development programmes, and provide opportunities for educators to improve and maintain qualification in the field of financial and tax literacy. Until now, schools in Lithuania have taught financial and tax literacy on an irregular basis, while the quality of development depended on the educator's motivation, involvement, and interest in this subject. To coordinate the institutions' efforts, a Coordination Committee for Financial Education is being set up.

National Plan for Financial Education in Portugal[78]

In Portugal, the three financial supervisors (the Central Bank of Portugal, the Portuguese Securities Market Commission and the Insurance and Pension Funds Supervisory Authority) recognise financial literacy in their mandate under the scope of conduct of business supervision. They established a partnership with a broad set of entities (including government ministries, financial sector associations, consumer associations, corporate associations and trade unions) to develop financial education initiatives under the National Plan for Financial Education[79].

This National Plan was created in 2011 and was revised in 2016 to include digital financial literacy as one of the priorities for the period 2016-2020, "to deepen knowledge and skills in using digital financial services".

The Central Bank of Portugal also establishes digital financial literacy as one of its strategic goals according to its Strategic Plan for 2017-2020. This is conducted as part of its financial consumer protection mandate by the Banking Conduct Supervision Department.

Money Wise Platform in the Netherlands

In the Netherlands, the Money Wise Platform (Wijzer in Geldzaken) is an initiative of the Dutch Government that aims to raise financial awareness. Set on promoting responsible financial behaviour, the strategy of the Money Wise Platform includes digital financial literacy. [80]

Participants in the platform are financial institutions, schools, scientists and consumer organisations. All these partners work together to raise financial awareness.

Supervisory authorities in charge of digital financial literacy strategy

In the majority of jurisdictions, the digital financial literacy strategy is conducted by national supervisory authorities. Some jurisdictions stated that it is conducted by central banks, commercial banks, banking industry organisations or specific research centres.

[78] "Todos contam" stands for "Everybody Counts" in English.

[79] http://www.todoscontam.pt/pt-PT/Principal/Paginas/Homepage.aspx.

[80] https://www.wijzeringeldzaken.nl/bibliotheek/media/pdf/7158-wig-strategic-programme-web-eng.pdf.

Financial information offers in Germany

BaFin has published numerous information products for consumers on its homepage (also on the topic of "digitalisation and FinTechs"). In addition to BaFin, there are several government agencies in Germany offering financial information, sometimes in cooperation with the industry – the Deutsche Bundesbank, the Federal Ministry of Justice and Consumer Protection in cooperation with the Institute for Financial Services, as well as various financial consumer protection actors, like "The Financial markets watchdog".

Bank of Mauritius in partnership with local authorities, universities and the media

The Bank of Mauritius has retuned its financial literacy strategy to focus on the digital dimension of the banking and finance world. Partnerships are also envisaged with local authorities, universities and the media to optimize dissemination of information and to gather feedback on impact of campaigns and new elements to be included in the strategy, as and when this will be required.

Training sessions on digital financial services in Brazil

In June 2017, the Central Bank of Brazil launched an on-line training platform to train collaborators from independent general consumer protection agencies scattered across the country. Topics include traditional and digital financial services regulation and tips on how to assist consumers who seek help and how they can avoid risky financial situations in the future.[81]

The Central Bank of the Republic of the Philippines' role in a financial literacy strategy

Since 2010, the Central Bank of the Republic of the Philippines (CBRP) has implemented a comprehensive Economic and Financial Learning Programme. This initiative consists of various learning events targeting specific audiences and delivered in different areas of the country.

The CBRP conducts its own financial literacy campaign. In addition, other financial sector regulators which comprise the Financial Sector Forum are contemplating similar strategies as part of their work in the FSF-Consumer Protection and Education Committee. The CBRP conducts information and

[81] http://www.cidadaniafinanceira.bcb.gov.br/edasuaconta/

awareness campaigns about risks and benefits of electronic products and services (e.g. important considerations when trading online, helpful tips on how to avoid financial fraud and scams channelled through digital means). These campaigns are delivered through the CBRP's official website and social media sites; printed primers; and onsite, structured financial learning seminars.

The CBRP will increasingly use digital and social platforms (e.g. PisoLit on Facebook) to deliver financial education messages. The CBRP, the Financial Inclusion Steering Committee (FISC) and other agencies also post financial education messages and advisories on their official websites and social media accounts. Moreover, some agencies like the Commission on Filipinos Overseas (CFO) have developed APPs focusing on financial education. While these initiatives are part of the financial education pillar of the National Strategy for Financial Inclusion, there is no specific, separate strategy for digital financial literacy.

Dissemination of the features and risks of digital payment services based on supervisors' information

Given its dual mandate, the Financial Consumer Agency of Canada, given its dual mandate, may leverage information (which could relate to digital payment services) by way of its supervisory function, as well as its consumer education and financial literacy function. Estonia reported that the Estonian Financial Supervision Authority provides annual statistics, which may be used in the work of bodies responsible for financial literacy. In France, the Banque de France and the Autorité de Contrôle Prudentiel et de Résolution regularly exchange information on digital payment services and other topics. While the majority of respondents have not adopted this practice, some respondents indicated their jurisdictions are progressing in that direction.

Initiatives to promote precautionary attitudes

Precautionary attitudes among users of digital payment service are promoted by financial literacy bodies in some jurisdictions. For instance, in South Korea, the Financial Supervisory Service makes an effort to prevent electronic financial fraud in many ways, such as developing and distributing videos or providing education programmes.

3. KEY TAKEAWAYS

- ***Adequate legal and regulatory framework***

  The legal and regulatory supervisory framework should encompass payment services with a specific emphasis on security principles and rules to ensure consumer protection. Conduct of business supervisors should have a clear mandate to oversee the mitigation of security risks and to develop a risk-based methodology. Supervisors should accomodate technology and innovation (SupTech) in their activities, relying on IT and new methodologies to strengthen their effectiveness. IT specialists should make part of supervisory teams and supervisors need to grant training to teams responsible for supervising digital payments.

- ***Ongoing and comprehensive monitoring of the main risks***

  The monitoring of the payments market and its evolution should be considered a task to be pursued by conduct of business supervisors. To this end, supervisors need to put in place different kinds of initiatives, with emphasis on mandatory reports and/or surveys to PSPs. Launching surveys targeting digital payment services' users could also be an effective way to collect information on the usage of innovative payments and precautionary measures to mitigate security risks.

- ***Close cooperation between supervisors and other relevant entities***

  The digitalisation of the payments market necessitates a collaborative supervisory approach. At the national level, conduct of business supervisors, prudential supervisors and payment overseers should work together to guarantee a secure, reliable and well-functioning payment system, taking into consideration consumer protection. Supervisors should also cooperate with public administration, telecommunication operators, and cybersecurity agencies. Information sharing is fundamental to reduce vulnerabilities and to better shield national infrastructures from threats. Cross-border provision of payment services and the global nature of security threats call for international cooperation.

- ***Close supervision of PSPs' disclosure of information***

  PSPs should disclose information on the features of the payment services they offer and their specific risks, and security procedures to be adopted by payment users. Conduct of business supervisors should oversee the completeness and adequacy of the information to ensure that users can make enlightened decisions. The mandatory disclosure of a KID, highlighting the digital payment services' features and risks, may be considered an effective supervisory practice that will lead to greater consumer knowledge and protection.

- ***Ongoing assessment of security risks through supervisory tools***

  The evolving digital ecosystem brings new risks, particularly security risks that conduct of business supervisors also need to address to ensure consumer protection. Security risks are perceived as among the most significant factors discouraging consumers from using digital financial services, especially digital payments. Conduct of business supervisors should have a wide range of oversight tools based not only on inspections, but also on complaints handling. The use of complaints data enhances the supervisory capacity of security mechanisms

adopted by PSPs. The effectiveness of the different oversight tools, especially complaints handling, requires an adequate regulatory framework setting out necessary competencies for conduct of business supervisors.

- ***Promotion of awareness campaigns on security risks***

  Awareness campaigns focusing on risks and security precautions to be adopted by users help to mitigate security risks and bolster consumers' confidence. Conduct of business supervisors may incorporate within the scope of their mission the promotion of awareness campaigns on risks raised by digital payments. Awareness campaigns may be launched by supervisors alone or in cooperation with other bodies, using different channels. Digital channels (e.g. dedicated websites) may be considered an effective vehicle to broadly distribute information on security risks to consumers.

- ***Promotion of digital financial literacy***

  The empowerment of users is also crucial to mitigating security risks. Supervisors play a key role in promoting precautionary measures by users by conducting financial literacy initiatives even when they do not have a specific mandate to do so. In cooperation with national literacy bodies, conduct of business supervisors can also play an important role to further promote the adoption of precautionary attitudes and safety procedures by users.

Digital financial services remain at the top of the agenda*.* The supervisory practices adopted across jurisdictions identified in this report confirm that conduct of business supervisors are committed to facing the challenges posed by online and mobile payments. Ensuring consumer protection irrespective of the channel through which the financial services are provided is at the top of the conduct of business supervisors' agenda.

Recognising the importance of sharing best practices to strengthen consumer confidence and reduce consumer risk, FinCoNet wishes to encourage discussion in the context of international fora on digital financial services.

This report is the second FinCoNet has issued on the topic of online and mobile payments. Representing the organisation's contribution to a that must continue, both of these reports highlight security issues. The first report identifies conduct of business supervisory challenges, proposing examples of actions to be taken. This latest report presents an in-depth analysis of supervisory practices adopted by a large and diverse set of countries to tackle the challenges identified, and to mitigate security risks.

4. ANNEX I

RESPONDENTS

Angola	National Bank of Angola
Armenia	Central Bank of Armenia
Brazil	Central Bank of Brazil
Canada	Financial Consumer Agency of Canada Autorité des Marchés Financiers of Quebec
Chile	Superintendency of Banks and Financial Institutions
Estonia	Estonian Financial Supervision Authority
France	Autorité de Contrôle Prudentiel et de Résolution
Germany	Federal Financial Supervisory Authority (BaFin)
Indonesia	Indonesia Financial Services Authority
Ireland	Central Bank of Ireland
Italy	Bank of Italy
Japan	Financial Services Agency
Lithuania	Bank of Lithuania
Luxembourg	Commission de Surveillance du Secteur Financier
Macedonia	National Bank of the Republic of Macedonia
Mauritius	Bank of Mauritius
Mozambique	Bank of Mozambique
Netherlands	Authority for the Financial Markets

Norway	Financial Supervisory Authority of Norway
Peru	Superintendency of Banks, Insurance and Pension Funds
Philippines	Central Bank of the Republic of the Philippines
Poland	Polish Financial Supervision Authority
Portugal	Central Bank of Portugal
Russian Federation	Central Bank of the Russian Federation
Singapore	Monetary Authority of Singapore
Slovakia	National Bank of Slovakia
South Africa	South African Reserve Bank
South Korea	Financial Services Commission
Spain	Bank of Spain
United Kingdom	Financial Conduct Authority
European Union	European Commission

5. ANNEX II

QUESTIONNAIRE – LAYOUT

FINCONET STANDING COMMITTEE 3

Questionnaire for conduct of business supervisors – Mitigating security risks with actions proposed in the FinCoNet report, 'Online and mobile payments: supervisory challenges to mitigate security risks'

June 2017

Introduction

1. After the 2014 FinCoNet Annual General Meeting (AGM) in Shanghai, FinCoNet members decided to set up Standing Committee 3 (SC3) to work on supervisory challenges related to online and mobile payments. SC3, led by the Bank of Portugal and with members from Brazil, Canada, China, Japan, South Africa and the UK, decided to focus on security risks.

2. FinCoNet SC3 released its report, 'Online and mobile payments: supervisory challenges to mitigate security risks'[82], on September 2016.

   The report assesses the findings of desk-based research and 27 responses to the FinCoNet survey of the same name from jurisdictions covering all continents. It focuses on how regulators and supervisors are responding to emerging risks, particularly security risks, and are keeping up with the pace of innovation. It also looks at issues that must be addressed in order to increase consumer trust and confidence in new digital payment systems. Finally, it identifies and sets out next steps, including examples of actions to be taken by supervisors.

3. Following the release of the report, FinCoNet SC3 established bilateral contact with FinCoNet observers, other international organisations and FinCoNet non-member jurisdictions that provided their comments and views on the report's proposed supervisory approaches and examples of actions to enhance consumer protection and mitigate the security risks of online and mobile

[82] Available at http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf.

payments. On receiving comments from the World Bank, the FinCoNet SC3 report was updated to include this new challenge: having an adequate legal and regulatory framework for fostering effective supervision.

4. The FinCoNet SC3 report was presented at the recent FinCoNet AGM in Jakarta in November 2016. In light of the rapid evolution of the digital ecosystem and associated challenges for supervisors, FinCoNet members agreed to continue work on online and mobile payments, implementing to the next steps proposed in the SC3 report. Given the fact that digital services can easily be accessed across borders, it was also decided that the Japanese survey on cross-border transactions would be included in SC3's further work. The membership of SC3 was also enlarged to include representatives from Australia, Indonesia and Mauritius.

5. During a conference call on February 9, 2017, FinCoNet SC3 members agreed to foster collaboration between FinCoNet and relevant international *fora*. The objective of collaborating in this way would be to widen the discussion regarding digital payment services, and to monitor the implementation of SC3's next steps and examples of actions by conduct of business supervisors (pages 13 and 14 of the report). To pursue this aim, it was also decided that a questionnaire would be drafted.

6. The draft questionnaire was presented and discussed at the FinCoNet Seminar and Open Meeting on April 7, 2017 in Dublin.

7. Incorporating references to actions proposed in the FinCoNet report, the questionnaire is a fact-finding exercise to identify effective and, potentially, innovative supervisory approaches regarding the mitigation of security risks in the digital ecosystem. FinCoNet SC3 will use responses to the questionnaire to develop a list of effective and comprehensive approaches to mitigating security risks in the digital context.

8. The questionnaire contains a set of yes/no questions and an optional 'In progress' column for actions currently being considered or under development. There is also a 'Comments' column where respondents may identify examples of actions taken in their jurisdictions to mitigate security risks of online and mobile payments. The 'Comments' column may also be used to refer to websites or reports offering further details on particular initiatives or experiences. To ensure that findings are comprehensive, the questionnaire includes an open question on initiatives not included in the monitoring questions. Finally, the questionnaire also includes a question that allows respondents to identify any practice/initiative/line of action that they would like to highlight and that could be considered an effective or innovative supervisory approach to mitigate security risks in the digital ecosystem and that may be presented as a case study.

9. In summary, the Questionnaire for conduct of business supervisors – Mitigating security risks with actions proposed in the FinCoNet report, 'Online and mobile payments: supervisory challenges to mitigate security risks':

- is an exercise to allow FinCoNet SC3 to identify effective and innovative supervisory actions;
- is not used for comparative or evaluation purposes, but it does provide jurisdictions with an opportunity to share initiatives and experiences on the status of implementation of actions proposed in the FinCoNet report; and
- is designed as a tool to help FinCoNet SC3 identify effective and innovative approaches related to policy options and priorities to support effective and comprehensive supervision and mitigation of security risks in the digital ecosystem.

Challenge 1

Having an adequate legal and regulatory framework to foster effective supervision.

Given the pace of developments in innovation within the financial services sector, conduct of business supervisors may incorporate in their scope of activities the oversight of online and mobile payments. The adopted supervisory approach may take into consideration the idiosyncrasies and specific risks of the digital ecosystem. Supervisors may also make use of technology to oversee the provision of online and mobile payments, when appropriate.

Monitoring questions	**Yes**	**No**	**In progress**	**Comments**
1.1. Do you have, in your jurisdiction, a specific mandate to oversee the provision of digital payment services?	☐	☐	☐	
1.2. Do you have a specific risk-based approach to supervision of digital payments services in place?	☐	☐	☐	
1.3. Do you use innovation and technology (SupTech) to prevent or mitigate security risks?	☐	☐	☐	
1.4. Do you provide specific training for the supervisory team responsible for overseeing digital payments?	☐	☐	☐	
1.5. Do you have IT specialists working in conduct of business supervision?	☐	☐	☐	

1.6. Do you implement other initiative(s) to address Challenge 1? If so, what are they?

Challenge 2

Ongoing and comprehensive monitoring of the main risks related to innovative payment services.

When monitoring the payments market, conduct of business supervisors may assess the development of digital payments and the main security incidents, thus considering payments by channel.

Monitoring questions	Yes	No	In progress	Comments
2.1. When monitoring the main security incidents, do you have a specific approach depending on the channel used?	☐	☐	☐	
2.2. Do you survey payment service providers (PSPs) on security risks and precautionary measures to mitigate them?	☐	☐	☐	
2.3. Do you survey payment service users on security risks and precautionary measures to mitigate them?	☐	☐	☐	
2.4. Do you require mandatory reports on security incidents from PSPs?	☐	☐	☐	
2.5. Is there a regular exchange of information on security incidents among national supervisory authorities (financial and non-financial sectors) in your jurisdiction?	☐	☐	☐	
2.6. Have you established a security alert system between supervisors, and PSPs?	☐	☐	☐	
2.7. Do you implement other initiative(s) to address Challenge 2? If so, what are they?				

Challenge 3

Close cooperation between conduct of business supervisors and prudential supervisors, payment systems overseers and other relevant entities at domestic and international levels, aimed at continuous information-sharing regarding security incidents and risk mitigation initiatives.

Conduct of business supervisors may encourage the setting-up of multidisciplinary groups – made up of prudential supervisors, payment systems overseers and other relevant entities − to discuss security incidents and actions to mitigate security risks.

Monitoring questions	Yes	No	In progress	Comments
3.1. Do you have a multidisciplinary formal group (set up or) led by the Government focused on digital payments and security issues?	☐	☐	☐	
3.2. Have you set up an (in)formal partnership focused on security risks with other relevant entities at a domestic level? If yes, specify the entities.	☐	☐	☐	
3.3. Have you set up an (in)formal platform for exchanging information and/or reacting to security incidents?	☐	☐	☐	
3.4. Are you a member of any international *fora* to exchange information and cooperate with supervisors, overseers and other relevant entities on security issues? If yes, which one(s)?	☐	☐	☐	
3.5. Do you have a National Payments Council in your jurisdiction?	☐	☐	☐	
3.6. Do you exchange information regarding security incidents with foreign financial supervisory authorities or with international organisations?	☐	☐	☐	

3.7. If a foreign payment service user suffered a loss or was defrauded/scammed through a cross-border payment service provided by a PSP authorized in your jurisdiction, can you take administrative actions (enforcement) or apply other penalties against the PSP in your jurisdiction? If yes, what kinds of administrative actions or penalties are requested by other jurisdictions?	☐	☐	☐	
3.8. If a payment service user in your jurisdiction suffered a loss or was defrauded/scammed through a cross-border payment service provided by a PSP authorised in another jurisdiction, do you have supervisory procedures/powers to act? If yes, please identify what kind of supervisory actions or operations did/can/will you take.	☐	☐	☐	
3.9. Do you implement other initiative(s) to address Challenge 3? If so, what are they?				

Challenge 4

Close supervision of PSPs to ensure the implementation and adoption of rules leading to the disclosure of the features of each payment service, their specific risks and the security procedures available to the user in relation to each payment transaction.

Conduct of business supervisors may oversee PSPs' disclosure of information to users on features of each payment service, on the risks and security procedures each time a user accesses any payment service.

Monitoring questions	Yes	No	In progress	Comments
4.1. Do you supervise the disclosure of digital payment services' features?	☐	☐	☐	
4.2. In your jurisdiction, are PSPs obliged to adopt a Key Information Document (KID)?	☐	☐	☐	
4.3. Do you pre-approve a KID regarding a specific digital payment service and its features?	☐	☐	☐	
4.4. Do you promote the off-site monitoring of PSPs' websites, home banking, apps, and other digital channels to assess their compliance with mandatory requirements on the disclosure of security risks and precautionary measures?	☐	☐	☐	
4.5. Have you developed specific measures to ensure the disclosure of information to payment service users on features, security risks and security procedures by PSPs?	☐	☐	☐	
4.6. Do you implement other initiative(s) to address Challenge 4? If so, what are they?				

Challenge 5

Ongoing assessment of security risks through the use of a variety of supervisory tools, particularly in respect to the management of complaints, to identify the most common and new security risks and their importance for consumer protection, allowing supervisors to promote targeted actions which could include the identification of regulatory gaps.

Conduct of business supervisors may promote the 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.

Monitoring questions	Yes	No	In progress	Comments
5.1. Do you use the information provided by complaints handling to identify security risks and plan risk mitigation initiatives?	☐	☐	☐	
5.2. Do you use the information provided by on-site inspections to identify security risks and plan risk mitigation initiatives?	☐	☐	☐	
5.3. Do you use the information provided by off-site monitoring to identify security risks and plan risk mitigation initiatives?	☐	☐	☐	
5.4. Have you recently proposed new regulations to offset regulatory gaps identified through supervisory tools? If yes, could you specify?	☐	☐	☐	

5.5. Do you implement other kind(s) of initiative(s) to address Challenge 5? If so, what are they?

Challenge 6

Promotion of awareness campaigns on the risks of digital payments, specifically regarding emerging security risks or major security incidents

Conduct of business supervisors may include in their mandate awareness campaigns on users' need to comply with security procedures and requirements that promote a balance between convenience and security. Supervisors may also include in their action the regular publication of information on features and risks regarding new digital payment services through booklets, flyers and online (website).

Monitoring questions	Yes	No	In progress	Comments
6.1. Have you run awareness campaigns and alerts focusing on the risks of digital payment services?	☐	☐	☐	
6.2. Have you run awareness campaigns on security precautions that digital payment service users should follow?	☐	☐	☐	
6.3. Do you publish content regarding security issues related to digital payment services on conduct of business supervisors' websites?	☐	☐	☐	

6.4. Do you implement other kind(s) of initiative(s) to address Challenge 6? If so, what are they?

Challenge 7

Coordinated approach between conduct of business supervisors and national bodies responsible for financial literacy to promote the use of precautionary procedures by digital customers.

Conduct of business supervisors may implement and/or collaborate closely with financial literacy bodies to further promote precautionary attitudes and security procedures by users, enhancing the impact and the dissemination of supervision-based information.

Monitoring questions	Yes	No	In progress	Comments
7.1. Is it legally mandatory for your jurisdiction to have a financial literacy body?	☐	☐	☐	
7.2. Does your jurisdiction have a digital financial literacy strategy?	☐	☐	☐	
7.3. Is your digital financial literacy strategy conducted by the national supervisory authority (or authorities)? If not, please specify the responsible entity (or entities), if any?	☐	☐	☐	
7.4. Does the financial literacy body (or bodies) disseminate information on the features and risks of digital payment services based on information provided by financial supervisors?	☐	☐	☐	
7.5. Does the financial literacy body (or bodies) run initiatives/campaigns to promote precautionary attitudes by digital payments services' users?	☐	☐	☐	

7.6. Do you implement other kind(s) of initiative(s) to address Challenge 7? If so, what are they?

Effective or innovative supervisory approaches mapping

Keeping in mind your responses to the above questions, would you like to highlight any additional practice/initiative/line of action that may be considered an effective or innovative supervisory approach to mitigate security risks in the digital ecosystem and that may be presented as a case study?