FinCoNet

INTERNATIONAL FINANCIAL CONSUMER PROTECTION ORGANISATION

Briefing Note

Supervisory challenges relating to the increase in digital transactions, especially payments

May 2022

Acknowledgements

FinCoNet would like to acknowledge the efforts of Standing Committee 3 (SC3) in developing this report and the survey that formed the basis of it. SC3 consists of representatives of Bank of Italy, Central Bank of Brazil, Financial Consumer Agency of Canada, Autorité des marchés financiers du Québec, French Prudential and Resolution Authority (ACPR), Otoritas Jasa Keuangan (OJK) – Financial Services Authority of Indonesia, Bank of Mauritius, Netherlands Authority for the Financial Markets, Central Bank of Portugal, Bank of Spain, and the UK Financial Conduct Authority. In particular, we would like to thank Magda Bianco, as Chair of the Standing Committee, her Bank of Italy colleagues Massimiliano Affinito and Rosario Grasso, as well as Francisco José Barbosa da Silveira, Giovani Gandini Giani, Marcelo Hiramatsu Azevedo, Teresa Frick, Vincent Gadbois, David Whalen, Fatine Afriany, Pascal Michaud, Gouro Sall Diagne, Samira Bourahla, Stephanie Machefert, A. Hudiyanto, Anto Prabowo, Yang Sultan Bestari, Aldi Firmansyah Rubini, Tilotma Gobin Jhurry, Tessa de Vries, Maria Carolina Campos, Mariana F. Fernandes, Carla Ferreira, Soraia Lopes, Ana Paula Neiva, David Pereira, Patrícia Pereira, Mariana Soares, Ana Cornejo, Yadira Grau, Javier Ortega, Tabitha Rendall and Sam Stoakes for their work in writing and producing the survey and report, and also to Matthew Soursourian, Laura Dunbabin, Anna Dawson, Sally Day-Hanotiaux and Miles Larbey, from the OECD Secretariat.

Finally, FinCoNet would also like to thank all respondents to the Survey on supervisory challenges relating to the increase in digital transactions (especially payments).

Disclaimer

This report is based on information and responses gathered between August and September, 2021. Information cited in this report has been updated to the furthest extent possible during the drafting process. Nonetheless, subsequent changes in circumstances and practices may render some information out-of-date.

The opinions expressed and arguments employed herein do not necessarily reflect the official views of FinCoNet member organisations.

About FinCoNet

In November 2013, FinCoNet was formally established as a new international organisation of financial consumer protection supervisory authorities. FinCoNet is recognised by the Financial Stability Board and the G20.

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.

Table of Contents

Figures

Boxes

Table of acronyms and abbreviations

AML	Anti-money laundering
ASIC	Australian Securities and Investments Commission
CFR	Council of Financial Regulators (Australia)
EBA	European Banking Authority
ECB	European Central Bank
EU	European Union
ISO	International Organization for Standardization
NFC	Near Field Communications
POS	Point of sale
PSD2	Payment Services Directive (Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market)
PSP	Payment services provider
SBS	Superintendencia de Banca, Seguros y AFP (Peru)
SC3	FinCoNet Standing Committee 3

Glossary

Term	Definition
Account information service provider	An online service to provide consolidated information on one or more payment accounts held by the payment service user with one or more payment service providers.
Banks	Banks are generally defined as institutions whose business is to receive deposits or other repayable funds from the public and to grant credits for its own account.
Contactless payments	Contactless payments allow users to make payment transactions without entering a PIN code, simply by placing a payment card (debit, credit and prepaid), a mobile telephone or another device (e.g., a smartwatch) near a POS terminal. NFC and Bluetooth are examples of contactless radio technologies.
Credit union	A credit union is a customer/member owned financial cooperative, controlled by its members, and operated for the purpose of maximizing the economic benefit of its members by providing financial services at competitive and fair rates.
Cybersecurity risk	Includes the risk of security incidents and the risks arising from consumer vulnerability to fraud and scams, covering phishing schemes and other types of social engineering, account hacking, data and identity theft, among others.
Digital ID	An identification system that uses digital technology throughout the identity lifecycle, including for data capture, validation, storage, and transfer; credential management; and identity verification and authentication.
Digital transactions/Digital payments	Transactions involving an electronic transfer of funds (including mobile payments, online payments, mobile wallets, apps, contactless payments and payments made with payment cards).
E-money	A monetary value stored electronically, including magnetically, represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer.
E-money institution	A legal person that has been granted authorisation to issue electronic money and provide a range of financial services related to payments.
Guidelines	Instructions – often non-binding – issued by a supervisory authority to be implemented by financial institutions according to existing legislation and regulation.
Innovation hub	Scheme via which firms can engage with the regulators and/or supervisors to raise questions and seek clarifications or non-binding guidance about FinTech related issues in the context of compliance with the regulatory framework, licencing or registration requirements, and regulatory and supervisory expectations.
Internet banking	A service that allows customers to access their bank accounts to manage their finances from the Internet.

Mobile banking	A service that allows customers to access their bank accounts to manage their finances via an app, phone, smartphone or tablet.
Mobile point of sale (mPOS)	A service that enables smartphones and tablets to accept payments.
Mobile wallets	Procedures agreed between the provider and the consumer to initiate a payment from linked payment cards or accounts, which can be accessed through devices connected to the internet or through mobile communication systems (such as NFC and Bluetooth). It can be incorporated in banking tools made available to the consumer by their bank, or offered by a third party.
National Payments Council	A coordination body established by central banks or other authorities to promote stakeholder collaboration in the payments industry.
Open banking	The sharing and leveraging of customer-permissioned data from banks and other entities with third-party developers and firms to build applications and services to provide more efficient and transparent options in banking.
Payment aggregators	A service provider through which e-commerce merchants can process their payment transactions. An aggregator allows merchants to accept different payment instruments such as credit card, bank transfers, e-money without having to setup a merchant account with a bank, card association etc.
Payment cards	Payment instrument issued by a payment services provider, used both to make payments and withdraw cash.
Payment initiation service	A service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.
Payment institution	A legal person that has been granted authorisation to provide and execute payment services.
Payment instruments	Any personalised device(s) and/or set of procedures agreed between the payment service user and the payment services provider and used by the payment service user to initiate a payment transaction (e.g. payment cards, home banking security credentials).
Payment services	Activities that include, namely (i) services enabling cash to be placed on a payment account; (ii) services enabling cash withdrawals from a payment account; (iii) execution of direct debits; (iv) execution of payment transactions through a payment card or a similar device; (v) execution of credit transfers; and (vi) money remittance.
Payment services providers (PSP)	Firms whose activity includes the provision of payment services referred above.
Platforms	Technology firms that facilitate interactions between two or more types of users (e.g., social media, e-commerce, etc.).

Pre-paid cards	Also called a stored-value card, a type of payment card not linked to a bank account. Instead, it can be loaded with funds and then used as a payment instrument.
Regulatory sandbox	Provides a special scheme, in which companies can test innovative financial products, services, or business models with actual customers in a controlled environment (a 'sandbox') pursuant to a specific testing plan agreed with the regulator and/or the supervisor and subject to the application of distinct safeguards.
Scams and frauds	Deceptive acts or operations aiming to gain a dishonest advantage, often financially. While the two terms are often used interchangeably, "scam" typically refers to the operation (e.g., "romance scam" or "investment scam") whereas "fraud" often refers to the fact of misrepresentation or the result of the scam (i.e., the acquisition of another person's property by deception).
Security incidents	Any attempted or actual unauthorised access, use, disclosure, modification, or destruction of information. Includes cyberattacks, systems failures or data breaches.
Social media payment options	Transfers of funds between individuals or from individuals to merchants through a social media network.
Supervisory letters	Official correspondence from a supervisory authority to a regulated firm. It can serve an educational purpose, i.e., to inform about the applicability of relevant legislation, rules, or guidelines and how they should be interpreted or applied in a specific situation. It may also serve as a warning, i.e., notifying a firm that they have violated a relevant rule under the supervisory authority's purview and that failure to remedy the violation may lead to enforcement action.
SupTech	Application and use of innovative or cutting-edge technology by supervisors to carry out their supervisory and surveillance work more effectively and efficiently.
Telco providers	Communications services providers specialising in telephone communications.

Executive summary

COVID-19 has accelerated the use of digital transactions. This brings both benefits and risks for consumers and supervisors. For consumers in particular, digital transactions, notwithstanding their greater convenience, are prime targets of financial scams and frauds.

This report's findings draw from 20 responses to FinCoNet SC3's "Survey on supervisory challenges relating to the increase in digital transactions (especially payments)", which was distributed to FinCoNet Members in August 2021 and was open for responses until September 2021.

This report aims to:

- Explore the impact of digitalisation and the increase in digital transactions — especially payments — since COVID-19 and, in particular, the impact on market conduct supervision;
- Provide an overview of the challenges for supervisors associated with cybersecurity risks and tackling financial scams; and
- Identify effective approaches that market conduct supervisors are employing to harness the benefits of digital transactions and mitigate the risks for consumers.

The following key findings emerge from this report:

Governance, frameworks and challenges

- In all responding jurisdictions, there is at least one authority responsible for the regulation and supervision of payments. This is most often carried out by a single authority such as a central bank. Cooperation arrangements regarding digital payments among different authorities are fairly common, even in jurisdictions where the responsibility is not shared.
- The most common types of payment providers subject to market conduct supervision are banks and payment institutions. Telco providers and platforms are less commonly subject to market conduct regulations.
- Four key challenges arise in the supervision of digital payments: vulnerability to cyber risks; vulnerability to frauds and scams; need to adapt regulation and supervisory practices; and lack of awareness among consumers.

Market conduct supervision tools & consumer awareness initiatives

- Authorities adopt a range of methodologies toward market conduct supervision of digital payments services. Two models were identified: risk-based classification of providers; and defined standards. For some authorities, market conduct supervision rules differ according to the payment channel used; in other cases the same requirements apply regardless of the distribution channel (digital or non-digital).
- Regarding supervisory tools, on-site inspections, off-site inspections and analysis of complaints data were deemed some of the most effective tools to detect misconduct in the field of digital payments. The COVID-19 pandemic has elevated the urgency of implementing remote supervisory activities, often using SupTech tools.

- Responding authorities ranked sending supervisory letters and issuing guidelines among the most effective corrective actions to take when misconduct has been detected.
- Authorities are now commonly employing staff with expertise in digital technologies, as well as providing specific technology-related trainings to the supervisory teams responsible for overseeing digital payments and conduct of business.
- Authorities are deploying communication strategies and campaigns to inform consumers about the characteristics and risks of digital payment services.

Security incidents, scams and frauds

- In most jurisdictions, the number of security incidents, scams and frauds linked to digital payments have increased in the past three years. The most commonly affected instruments/mechanisms are internet banking, mobile banking and payment cards.
- Among different consumer groups, frauds and scams most commonly affect seniors and/or newly retired people, retail investors, and immigrants.
- The most common sources used to monitor security incidents or scams and frauds are reports from PSPs and complaints data. Consulting with other authorities at a national level is also common for monitoring security incidents – less so for the purpose of monitoring scams and frauds.
- To track emerging security risks, authorities establish specific initiatives, such as data collection from supervised entities, public/private sector information sharing platforms, coordination with telco authorities, information sharing mechanisms with foreign regulators and international payment system networks. Emerging risks may also be monitored based on insights from innovation hubs and regulatory sandboxes established to foster technological innovation in the financial services industry.
- Authorities reinforce the importance of ongoing and comprehensive monitoring of security incidents, scams and frauds linked to digital payments, highlighting that reporting requirements by regulated entities are one of the most relevant information source used to monitor them. Moreover, authorities emphasised the relevance and utility of exchanging information about security incidents, scams and frauds with foreign financial supervisory authorities or with international organisations (such as FinCoNet).

The role of digital payments in consumer finance is growing fast. Market conduct supervisors need to be prepared to monitor new payment products, business models and providers, in order to stay abreast of the conduct risks, ensuring adequate conduct supervision and consumer protection.

1. Introduction and purpose of the report

1.1. Background

COVID-19 has accelerated the use of digital transactions. Consumers have turned to digital payments to manage their finances during lockdowns and to abide by social distancing policies. At the same time, governments have introduced measures to support the transition to greater digitalisation. Together, these factors have led to unprecedented adoption of digital payment services. This brings both benefits and risks for consumers and supervisors. For consumers in particular, digital transactions, notwithstanding their greater convenience, are prime targets of financial scams and frauds.

In this report, FinCoNet SC3 explores the impact of digitalisation and the increase in digital transactions— especially payments—since COVID-19 and, in particular, the impact on market conduct supervision. The report identifies effective approaches that conduct supervisors employ to harness the benefits of digital transactions and mitigate the risks for consumers. In particular, it considers challenges for supervisors associated with cybersecurity risks and tackling financial scams, which increased significantly in many jurisdictions since the outbreak of the pandemic.

FinCoNet's reflection on digital payments started in 2016. That year, FinCoNet SC3 published a report on *Online and mobile payments: Supervisory challenges to mitigate security risks*. Among other things, the report focused on how regulators and supervisors were responding to emerging risks, particularly security risks, on how they were keeping up with the pace of innovation, and on issues to be addressed in order to increase consumer trust and confidence in new digital payment systems. A categorisation of payment services was outlined and a set of conduct of business supervisory challenges related to digital payments were identified. In 2018, FinCoNet SC3 published a second report – *Online and mobile payments: An overview of supervisory practices to mitigate security risks* – which aimed to present the conduct of business supervisory practices or initiatives implemented across jurisdictions to mitigate security risks in the digital context.

Building on this previous work, and in accordance with the FinCoNet Programme of Work 2021-2022, FinCoNet SC3 developed a survey to gather insights related to supervisory challenges stemming from the recent increase in digital transactions. Responses to this Survey formed the basis of this report.

1.2. Overview of the survey

To prepare this report, SC3 developed the "Survey on supervisory challenges relating to the increase in digital transactions (especially payments)" (see Appendix B for the full text of the Survey), which was distributed to FinCoNet Members in August 2021 and was open for responses until September 2021.

The Survey consisted of four parts:

A) Governance, which included questions about which authorities were responsible for the supervision of digital payments and how they worked together;

B) Legal and Regulatory Framework, which contained questions about the relevant mandates, powers, regulations, and challenges related to digital payments;

C) Security Incidents, Scams and Frauds, which focused on monitoring, overseeing, and responding to security incidents, scams and frauds; and

D) Market Conduct Supervision Tools & Consumer Awareness Interventions, which contained questions about how authorities practically approached conduct supervision related to the provision of digital payments, including their use of SupTech tools, detecting misconduct, enforcement actions, and staffing issues.

The Survey was distributed to a large number of jurisdictions and representative bodies, including FinCoNet members and observers. A total of 20 participating authorities provided responses to the Survey (see Appendix A "List of responding authorities" for a full list of respondents).

1.3. Purpose and structure of the report

This report aims to:

- Explore the impact of digitalisation and the increase in digital transactions — especially payments — since COVID-19 and, in particular, the impact on market conduct supervision;
- Provide an overview of the challenges for supervisors associated with cybersecurity risks and tackling financial scams; and
- Identify effective approaches that market conduct supervisors are employing to harness the benefits of digital transactions and mitigate the risks for consumers.

The report is organised in the following chapters:

- Chapter 2 provides an overview of the authorities that are in charge of regulating and/or supervising digital payments and the way they interact with other relevant authorities and with the entities they regulate or supervise. It also covers the mandates, powers and functions of these authorities vis-à-vis digital payments, as well as the challenges related to digital payments.
- Chapter 3 reports on market conduct supervision tools and consumer awareness initiatives. It describes risk-based approaches to supervising digital payments, channel-specific approaches, use of SupTech tools, detecting misconduct, and corrective actions. It also includes findings on staff capacity, training and consumer outreach and financial and digital education initiatives.
- Chapter 4 covers security incidents, scams and frauds. It describes trends and targets, monitoring and reporting mechanisms, security tools, disclosure requirements, and coordination and information-sharing practices.
- Chapter 5 synthesises the key findings that can be drawn from this report and discusses the next steps regarding the work of SC3.

2. Digital payments: An overview of their governance, regulatory frameworks and challenges

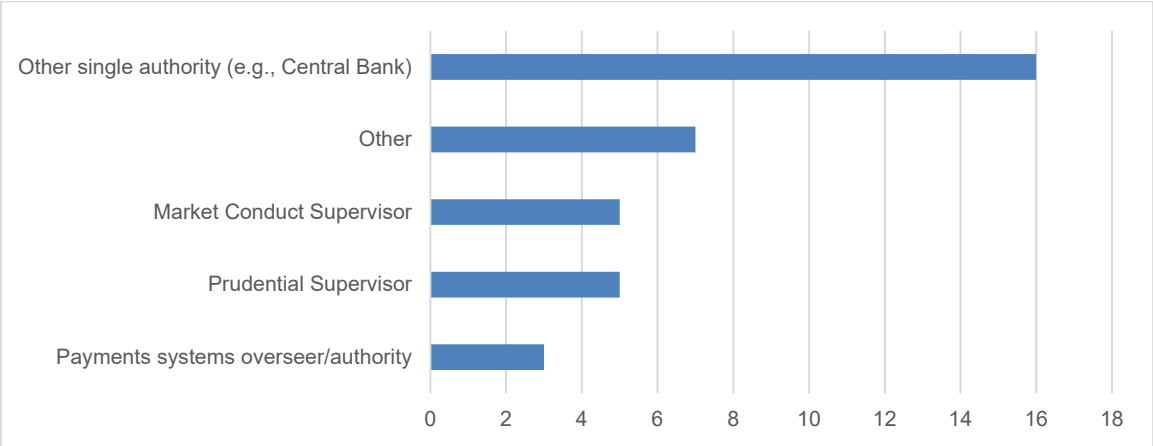
This chapter sets out the governance of payments, including the authorities in charge of regulating and/or supervising digital payments. It also describes how these authorities interact and share information with other institutions, as well as the mandates and powers of the authorities themselves. It provides an overview of the types of payment providers subject to market conduct supervision and the challenges related to supervising providers of digital payments.

2.1. Governance

All respondents indicated the presence of at least one authority in their jurisdiction responsible for the regulation and supervision of payments, including digital payments. However, the governance configurations are multiple – e.g., a central bank performing a dual prudential and market conduct oversight function, or performing one of the functions in collaboration with an authority performing the other function. Some respondents also cited roles for government ministries and competition regulators; others reported that two or more authorities share responsibility for regulating and supervising payments. It is worth noting that, while oversight of payment systems is a common feature among jurisdictions, dedicated payments systems overseers/authorities, as an independent/separated authority, are relatively uncommon.

A closer examination of authorities responsible for supervision of payments is provided in Figure 1 below.

Figure 1. Authorities responsible for the regulation and supervision of payments, including digital payments[1]



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

[1] In some jurisdictions, the single authority, for instance, the Central Bank, may integrate in the same structure the market conduct supervisor, the prudential supervisor and the payment system overseer.

2.2. Exchanging information and coordinating activity among authorities

As the regulation and supervision of digital payments may involve shared responsibilities among different authorities, establishing appropriate mechanisms for sharing information and coordinating activity is critical. According to the responses gathered, such mechanisms have been developed even in jurisdictions where the responsibility is not shared among separate authorities (e.g. establishing a cooperative framework between specialised Directorates/Departments within the same authority). Cooperation mechanisms may relate to payments in general or be specialised in digital financial services; cross-border issues may also be the focus area of cooperation. As concerns the legal frameworks for the exchange of information and activity coordination, common mechanisms include national councils established by regulation, informal agreements among authorities, administrative agreements, charters and memoranda of understanding, task forces and committees.

Inter-authority information-sharing bodies may either meet on a scheduled or ad hoc basis, typically multiple times per year. Information exchanged includes statistical data, best practices, financial operations standards and other information pertinent to the supervision of regulated financial institutions. Recent initiatives of selected inter-authority bodies are described in Box 1.

Mandates for inter-authority bodies focused on payments are quite varied and may aim at different objectives, e.g. financial stability and crisis management coordination, contributing to the development of standards for financial transactions (e.g., ISO 20022[2]), enhancing financial inclusion and improving public knowledge and safety when using payment services. As concerns specifically digital financial services, mandates cover issues such as cyber incidents, the enhancement of cyber security systems, the monitoring of market developments related to FinTech and related risks, the formulation of regulatory proposals, and, in certain instances, the development of joint training and outreach programs. While cross-border issues are relevant to the mandates of inter-authority bodies in several jurisdictions, these issues typically arise in the context of stability and operational concerns (e.g. the proper functioning and the evolution of regional payment systems), rather than in the context of financial consumer protection or market conduct supervision.

Box 1. Recent initiatives of inter-authority bodies

In **Australia**, the Council of Financial Regulators (the coordinating body for Australia's main financial regulatory authorities - CFR) reviewed the regulatory requirements that apply to stored-value facilities, i.e. a non-cash payment facility allowing the holder to store funds in a facility for the purpose of making future payments. Recommendations from the CFR's review were made to modernise the regulation of Australian payments companies and are currently being implemented.

Indonesia has established the Indonesian Payment System Forum, a forum of regulators comprising the Bank of Indonesia as payment system authority and other related regulators. The Indonesia Payment System Blueprint 2025 is designed to support activities in the digital economy and finance, to catalyse economic recovery, and to accelerate economic and financial inclusion.

[2] A single standardisation approach (methodology, process, repository) to be used by all financial standards initiatives.

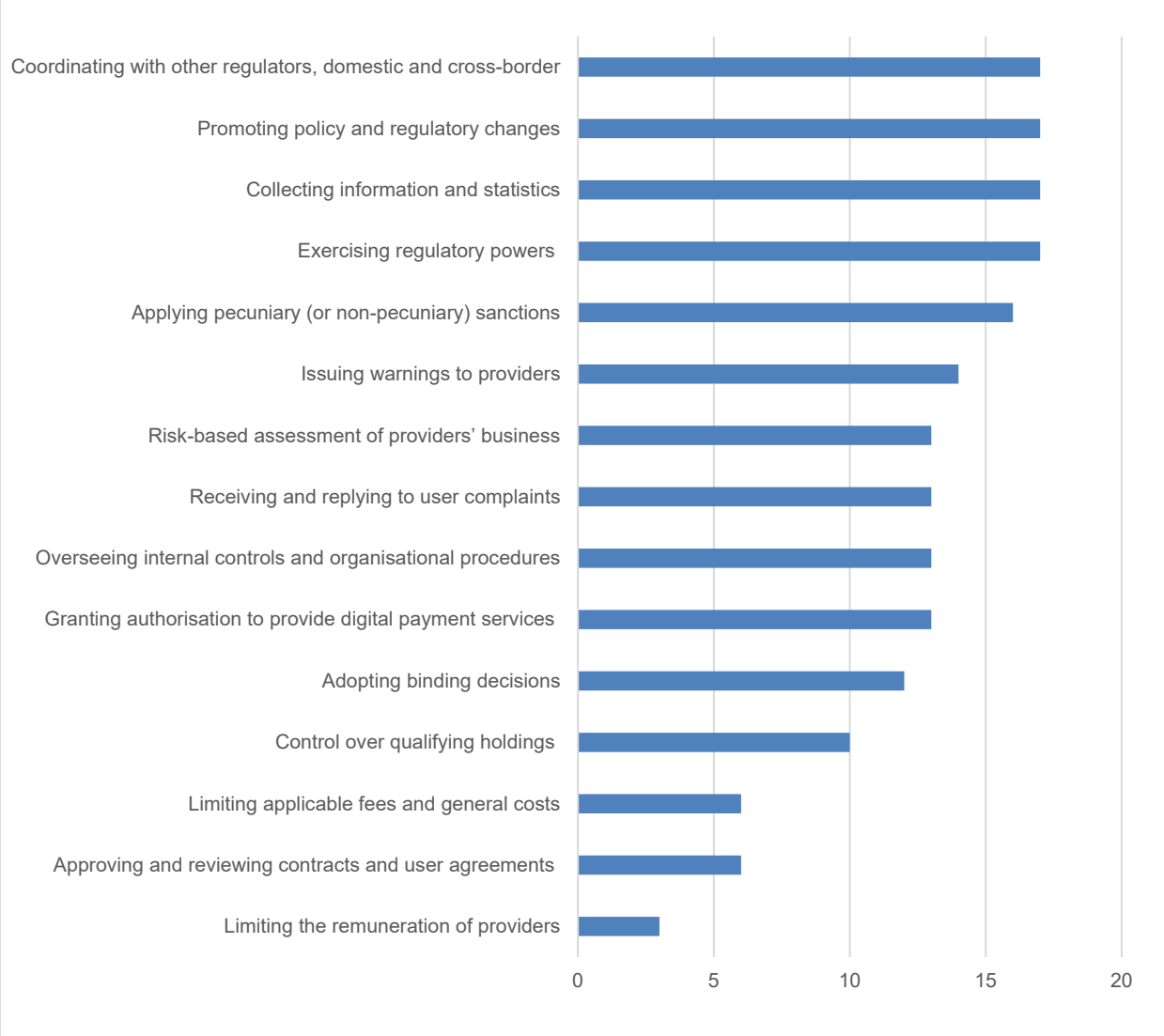
The **Italian** Payments Committee is a cooperation forum chaired by the Bank of Italy whose main objective is to foster the development of a secure, innovative and competitive market for private and public payments in Italy that is able to respond to global challenges and to meet the needs of users. The Committee has established an ad hoc working group to monitor the migration of service providers to new European Banking Authority (EBA) rules related to e-commerce payment card transaction security.

In **Portugal**, a National Council of Financial Supervisors ("Conselho Nacional de Supervisores Financeiros" - CNSF) was established by law (Decree-Law No. 228/2000) with the purpose of enhancing the coordination and sharing of information among financial supervisory authorities (Central Bank of Portugal, Securities Market Commission and the Insurance and Pension Funds Supervisory Authority) and formulating regulatory proposals on matters relating to the sphere of action of more than one of the supervisory authorities. In 2018, it created a Contact Group on FinTech, whose objective is to monitor the risks related to technological innovation in the financial sector. One of the lines of action is the assessment of the impact of digital transformation.

2.3. Mandates, powers and functions

Most respondents (N=15) cited a specific mandate to supervise the market conduct of digital payment service providers; furthermore, others indicated that this mandate is already covered by a broader responsibility for overseeing the financial system. The mandate to supervise the market conduct of payment providers includes different powers and functions. These powers and functions are presented in Figure 2 below. In general, conduct supervisors dispose of a wide variety of powers and functions, for instance, to coordinate with other regulators, to promote policy and regulatory changes, to collect information and statistics, to exercise regulatory powers, to apply pecuniary (and non-pecuniary) sanctions, among others.

Figure 2. Powers and functions included in the mandate to supervise market conduct of digital payment services providers

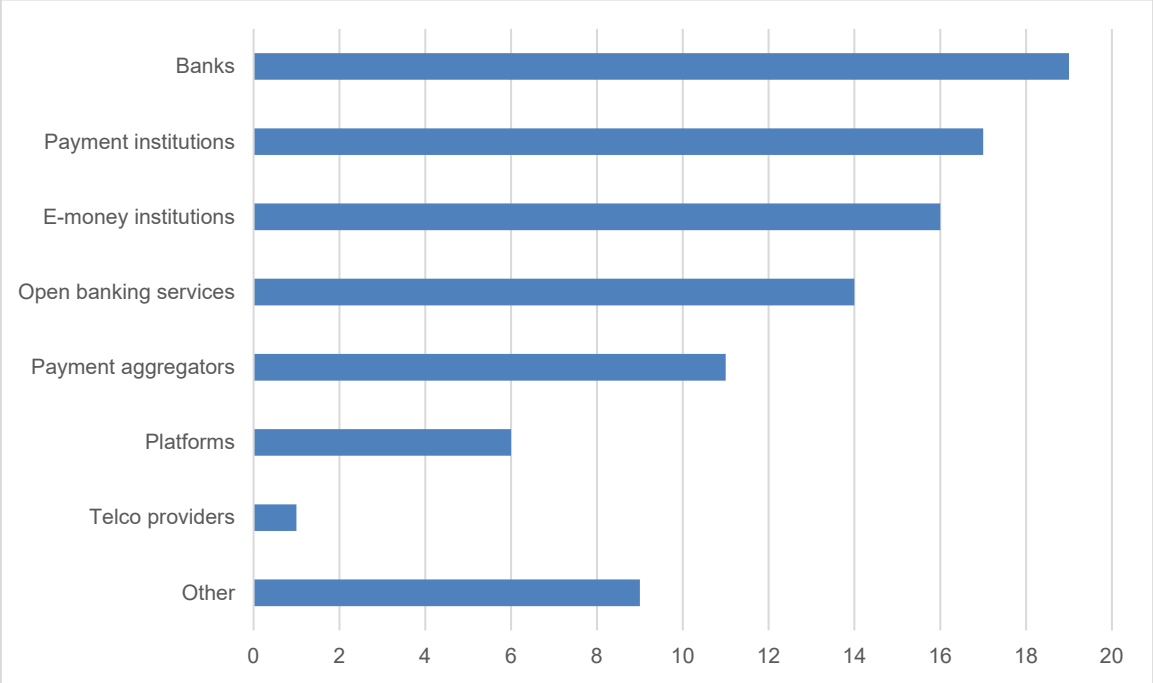


Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

2.4. Payment providers subject to regulation

Technological improvements, coupled with the growing demand for digital payments, are increasingly reshaping the way payments are made. The COVID-19 pandemic increased the take-up of e-commerce and online service and also catalysed demand for digital payment methods. The providers of such payment methods vary across jurisdictions, as do whether they are subject to market conduct regulation. A closer examination of payment providers subject to regulation is detailed in Figure 3 below, which shows that banks, payment institutions and e-money institutions are the payment providers most commonly subject to market conduct regulation. Telco providers and platforms are less commonly subject to market conduct regulations.

Figure 3. Payment providers subject to market conduct regulation



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

It is worth noting that other payment providers subject to regulation are quite diverse, and may include payment initiation service providers, payment card network operators, credit unions and postal service providers, exchange houses, insurance companies, as well as crypto custody business services and certain providers using distributed ledger technology systems.

Some jurisdictions have function or activity-based regulation in place, meaning entities providing payment services are subject to oversight regardless of their core industry; many have a legal and regulatory framework based on international or regional standards (most notably EU countries); others work with innovative FinTech entities, including payment service providers, to provide informal guidance on licensing and regulation (entity-based approach).

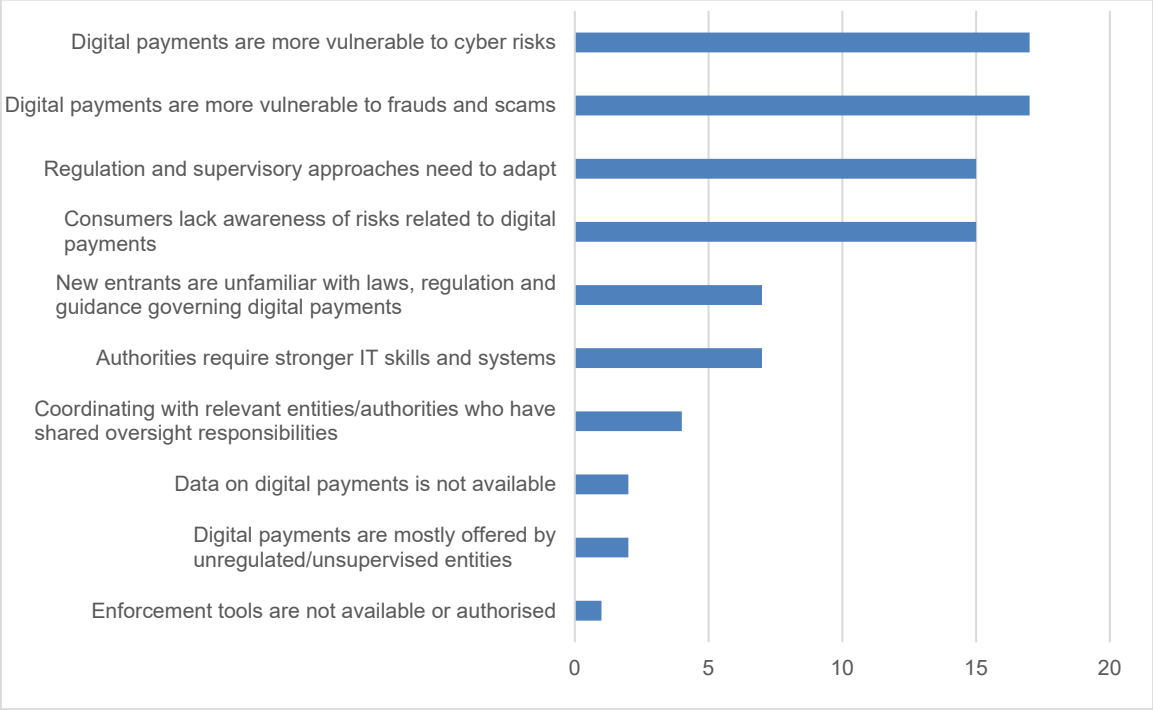
Providing payment services on behalf of a payment service provider

Most respondents (N=18) indicated that the applicable regulatory framework allows for third parties to provide payment services (e.g., agents, correspondents, cash-in/out outlets). A relevant number of respondents (N=13) reported that rules or regulations exist on the initiation of digital payment services by a consumer through a third-party entity - e.g. the European Payment Services Directive 2015/2366/EU (PSD2), applicable throughout the European Union, sometimes supplemented by additional legislation at national level. Specific legislation also exists in other jurisdictions, notably in some developing countries.

2.5. Challenges relating to digital payments and effective approaches to stay abreast of developments

Respondents reported a number of challenges, most notably those related to cyber risks, frauds and scams, as illustrated in Figure 4 below.

Figure 4. Primary challenges related to digital payments



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

A general consensus exists that sufficient information is available regarding payment trends and developments (as only two respondents selected "data on digital payments is not available"), with respondents noting a need to adapt regulation and supervisory approaches to the market (N=15). Lack of enforcement tools did not emerge as a significant challenge for many respondents (N=1).

A number of mechanisms were reported to be effective in order to stay abreast of developments related to digital payments, including regularly consulting with market participants; exchanging information with supervisory authorities from different jurisdictions; participating in international groups and initiatives related to digital payments; and setting up an innovation hub or a regulatory sandbox.

3. Market conduct supervision tools & consumer awareness initiatives

This chapter provides an overview of the tools used by market conduct supervisors in the context of digital payments. It describes how they use SupTech and other methods to assess risk and detect misconduct, including through channel-specific approaches. It also includes findings on corrective actions, staff capacity and training, consumer awareness initiatives and financial education.

3.1. Risk-based approach

Risk-based supervisory approaches require supervisors to systematically prioritise their activities focusing on the most important risks. Such an approach may include developing a consistent evaluation framework, assessing and ranking risks, monitoring and identifying emerging risks, and deciding how to assign resources and organise the authorities' activities based on its perceived risks.

In this context, 10 responding authorities reported having in place a specific risk-based approach for the market conduct supervision of digital payments services.

Models

Based on the answers provided to the survey, two different models can be found - which may work in tandem. Examples are set out in Box 2. In addition, some supervisors also rely on a self-assessment approach, whereby PSPs are themselves required to establish internal compliance systems using a risk-based self-assessment.

Model 1 - Risk-based classification of providers

- The supervisory measures applicable to digital payment service providers is grounded on a risk profile calculation carried out within the risk-based supervisory approach on the basis of quantitative, qualitative and functional characteristics of their activities, such as size of the subject, volume and number of operations, infrastructure, relationships with other subjects. In such approach, various sources of information, such as databases of operations of the supervised entities, are complemented by consumer complaints and social media mentions.

Model 2 - Defined standards

- There are general conduct supervision obligations relevant to the prevention of fraud, scams and security incidents. While there are no mandatory provisions that establish what each supervised entity needs to do to meet those standards, general guidance on these matters is provided by authorities as well as some proactive and reactive monitoring depending on risk-based evaluation.

Box 2. Specific risk-based approaches adopted by Bank of Italy and the Superintendence of Banking, Insurance and Private Pension Fund Administrators (SBS) of Peru

Bank of **Italy** has in place a specific risk-based approach to market conduct supervision of digital payments services based on PSD2 provisions, as transposed into the Italian banking law and the authority's implementation provisions (such as Provisions on Transparency). The involvement of financial institutions in the provision of payment services is taken into account by the Bank of Italy's internal model of classification of customer risk – a conduct supervision tool currently under development and testing – which aims to score financial institutions based on their business model and overall quality of the relations with customers.

The market conduct department of SBS of **Peru**, has in place a specific risk-based approach to market conduct supervision in which the requirements are associated with the size, management and complexity of operations of the companies of the supervised systems. As part of the supervision model, SBS analyses various sources of information, including consumer complaints and social media mentions regarding digital payment services; which are complemented by the databases of operations of the supervised entities; management plan and results; complaints report; transactional databases; inspection information and regulatory inquiries among others.

3.2. Channel-specific approaches

Just as supervisory approaches on digital payments may differ across jurisdictions, they can also vary within jurisdictions according to the digital payment channel used. Among respondents, however, only a minority (N=3) reported a specific approach to market conduct supervision depending on the channel used. Further information is set out in Box 3.

Box 3. Examples of differentiating approaches based on payment channel and instrument

Japan and **Canada** reported similar approaches, differentiating their conduct oversight on the characteristics of each payment system. These countries set out distinct market conduct requirements for the use and acceptance of different payment instruments or payment service providers, such as issuers of prepaid payment instruments and electronic payment services.

For example, The Code of Conduct for the Credit and Debit Card Industry in Canada sets out distinct market conduct requirements for the use and acceptance of credit cards, debit cards, as well as for the acceptance of contactless and mobile payments. Furthermore, Financial Consumer Authority of Canada (FCAC) Compliance Bulletin B-6 requires federally regulated financial institutions to conduct comprehensive investigations in instances where debit and credit card holders have alleged unauthorised use of their cards. Bulletin B-6 builds on market conduct requirements set out in the Cost of Borrowing Regulations (which pertain to credit cards), the Canadian Code of Practice for Consumer Debit Card Services (which pertain to debit cards), and the zero liability policies of the major payment card network operators. Federally regulated financial institutions issuing prepaid cards are subject to the Prepaid Payment Products Regulations, which set out

market conduct obligations for disclosure both at the point of sale and post-sale. Mandatory reporting requirements (e.g., aggregate complaint reporting) differ for federally regulated financial institutions and payment card network operators.

The **Australian** Securities and Investments Commission (ASIC) takes a flexible approach to conduct oversight obligations for digital payment service providers. As such, the regulation of a digital payment channel depends on the particular circumstances. Unless an exemption applies, non-cash payment facilities that allow users to load and store value are regulated by ASIC under the Corporations Act (noting there are exemptions for e.g., low-value non-cash payment facilities, loyalty and gift schemes and road tolls). Digital wallets, which allow for one or more separate product(s) to be 'linked' and used to make payments, may be non-cash payment facilities in their own right. Whether these wallets are regulated by ASIC depends on how they operate, and the rights and obligations associated with the wallet. For instance, if all payments initiated using a digital wallet are debited to a credit facility, then the wallet is not considered a financial product and a financial service license is not required (noting that the credit facility itself is regulated). The Australian government is currently conducting a review of Australia's payment systems regulation.

3.3. SupTech tools for digital payments

Among the 20 responding authorities, the implementation of SupTech tools for the supervision of digital payments is varied. Such tools have been deployed both to monitor risks and mitigate or prevent such risks.

Regarding SupTech tools to *monitor* risks to consumers stemming from digital payments, three responding authorities have already implemented such tools; six have not implemented such tools but had plans to; eight have not implemented such tools and do not plan to; and three did not provide a response to the question. Illustrative examples are set out in Box 4.

Box 4. SupTech for monitoring, reporting and analysis

Bank of **Italy** described a project called "RepTech" – still being developed - which uses social media data and natural language processing (of complaints) to define a global sentiment analysis score for each financial institution and a separate score for each area of interest for consumer protection (e.g., payment services).

The Bank of **Mauritius** started licensing Payment Service Providers effective from July 2021. Currently, regulatory returns are submitted through a manual process. The Bank of Mauritius is envisaging to use a RegTech tool for submission of regulatory returns by payment service providers to ensure compliance with reporting requirements and data integrity. For more efficiency in the analysis of data, the Bank of Mauritius is exploring available analytical solutions. The use of such tools will facilitate offsite supervision of the payment service providers and enable detection of early warning signals in their performance.

Financial Sector Conduct Authority of **South Africa** has a sophisticated AI social media sentiment monitoring tool, in relation to financial institutions including payments, that uses a human "crowd" to assess human subtlety that machines can't always manage well, and is programmed to be aligned to the evolving "treating customers fairly" (TCF) principles and

outcomes-based conduct law. In sum, it picks up and categorises social media sentiment towards specific providers or categories of providers, and applies a TCF lens.

Regarding SupTech tools to *prevent* or *mitigate* risks to consumers stemming from digital payments, three responding authorities have already implemented such tools; five have not implemented such tools but have plans to; nine have not implemented such tools and do not have plans to; and three did not provide a response to the question.

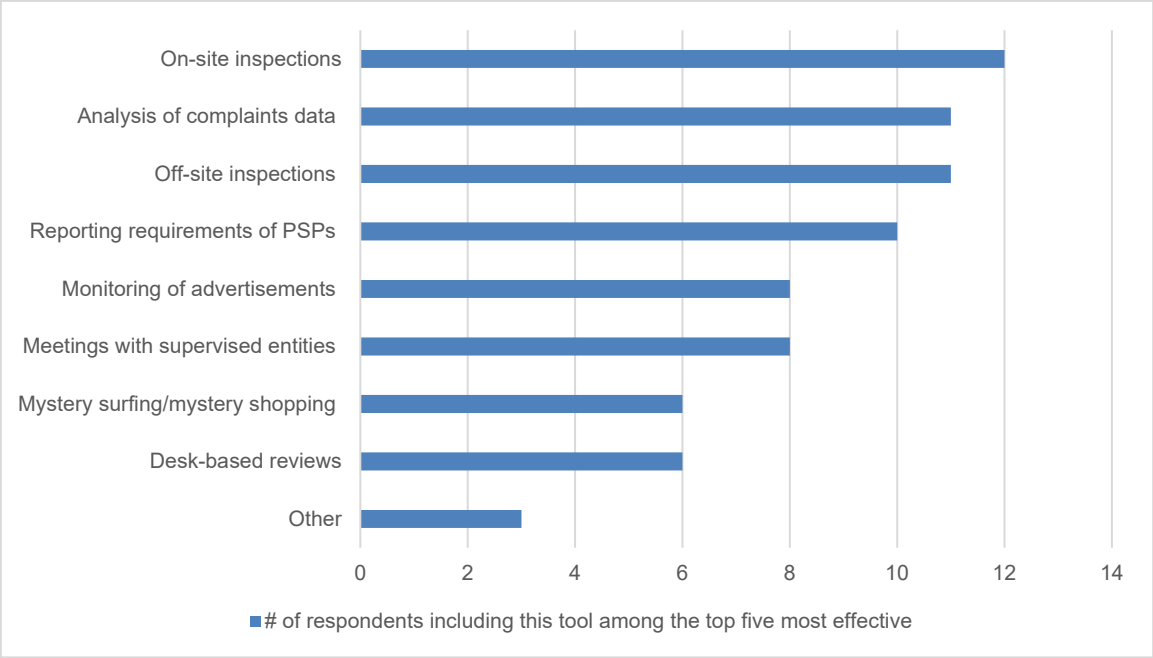
3.4. Assessing compliance and detecting and addressing misconduct

Responding authorities diverge on their approaches to monitoring the compliance of PSPs with mandatory disclosures of security risks and their implementation of required precautionary measures to prevent fraud, scams and security incidents. Some authorities monitor PSPs' websites online platforms, apps, and other digital channels to carry out these assessments. Others reported that they would only pursue this as part of a risk-based monitoring approach – for example, if specific complaints were addressed to the authority.

Supervisory tools used to detect misconduct

As shown in Figure 5, more than half of respondents (N=12) recognise on-site inspections as one of the most effective supervisory tools to detect misconduct in the field of digital payments, followed by analysis of complaints data (N=11) and off-site inspections (N=11). While 10 authorities deem reporting requirements of PSPs as one of the most effective supervisory tools to detect misconduct, it was also noted that these requirements are only as good as the usefulness of the data requested, and the quality with which it is provided.

Figure 5. Supervisory tools deemed to be the most effective to detect misconduct in the field of digital payments



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

Many respondents also use information from meetings with supervised entities and advertising monitoring to identify misconduct in digital payments.

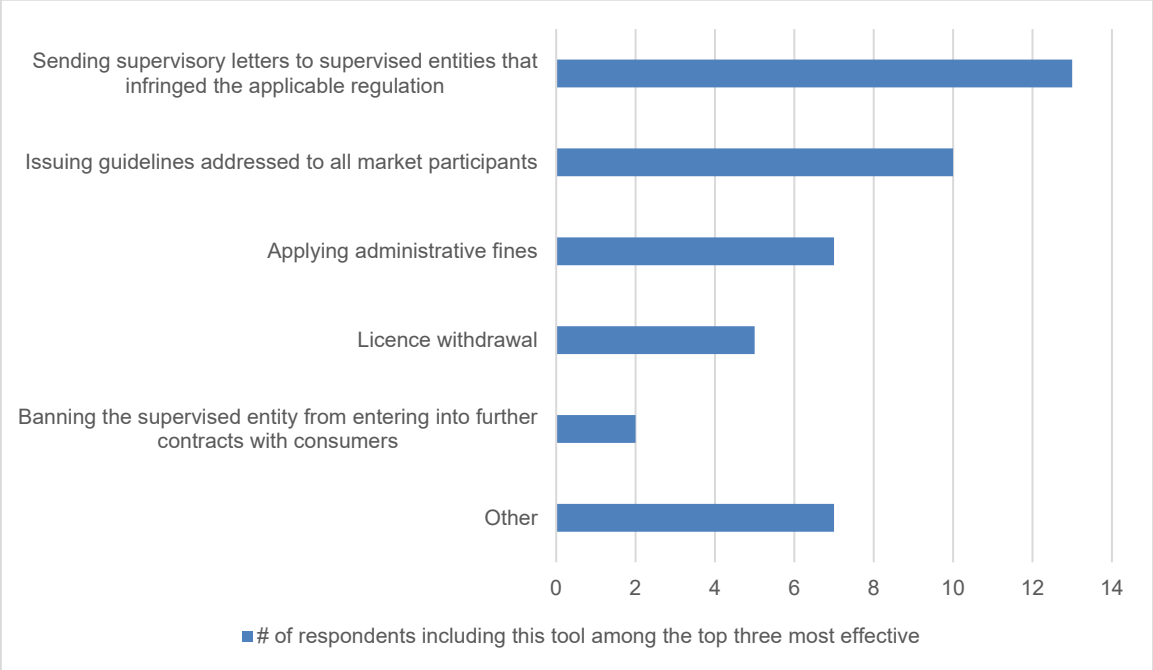
Information gathered from other authorities (for example on predatory scam behaviour), mandatory internal audit programmes, mandatory third-party assessment of compliance and protected disclosures were identified as additional tools by some respondents.

Notably, respondents reported that the COVID-19 pandemic had elevated the urgency of implementing remote supervisory activities, often using SupTech tools to address data collection and analysis issues including structured and unstructured digital data.

Corrective actions

Once a supervisory authority has detected misconduct by a PSP, they must determine how to address it. As illustrated by Figure 6, the three corrective actions identified as most effective to address misconduct in the field of digital payments are: (i) sending supervisory letters to supervised entities that infringed the applicable regulation; (ii) issuing guidelines addressed to all market participants and (iii) applying administrative fines.

Figure 6. Most effective corrective actions to address misconduct in the field of digital payments



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

Some respondents emphasised the importance of issuing guidelines, which are relevant to foster good business practices observed or to recommend in detail practices considered as appropriate, as well as to provide clear instructions on conduct of business, governance structures, responsibilities and accountabilities of the different parties involved.

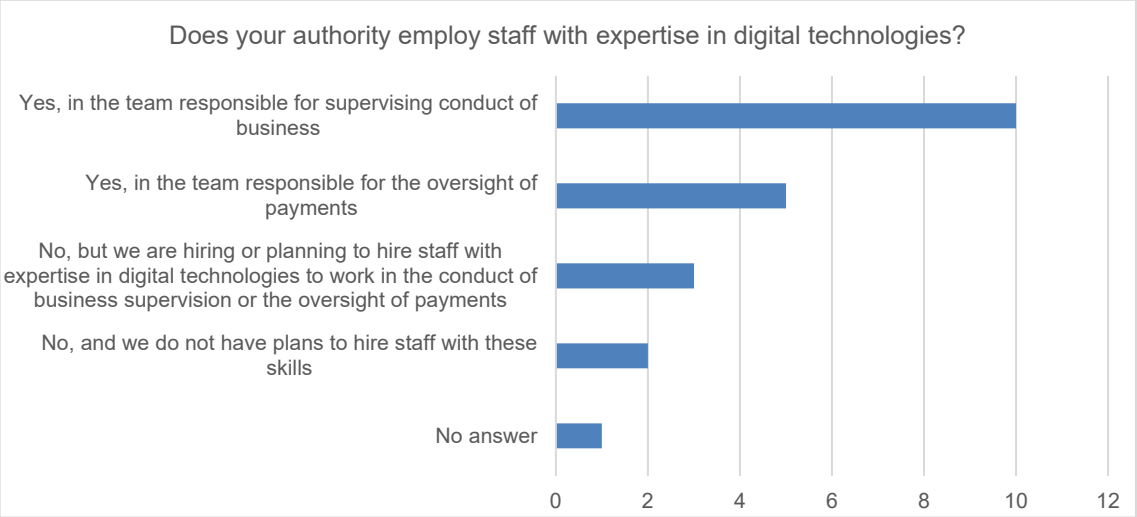
Additional corrective actions mentioned by respondents include: imposing bans on specific activities/products/clients/operations/etc.; hosting meetings with the supervised entities; issuing specific orders to correct irregularities found at a supervised entity; or entering into

a "cease and desist" agreement with the supervised institution under investigation. In the latter, the financial institution commits itself to cease and correct the irregularities reported and to fulfil corrective obligations, in addition to paying a pecuniary contribution, in exchange for the suspension or dismissal of the sanctioning administrative process.

Other regulatory tools used included engagement with industry and stakeholders, surveillance, education, and policy advice.

3.5. Staff capacity and training

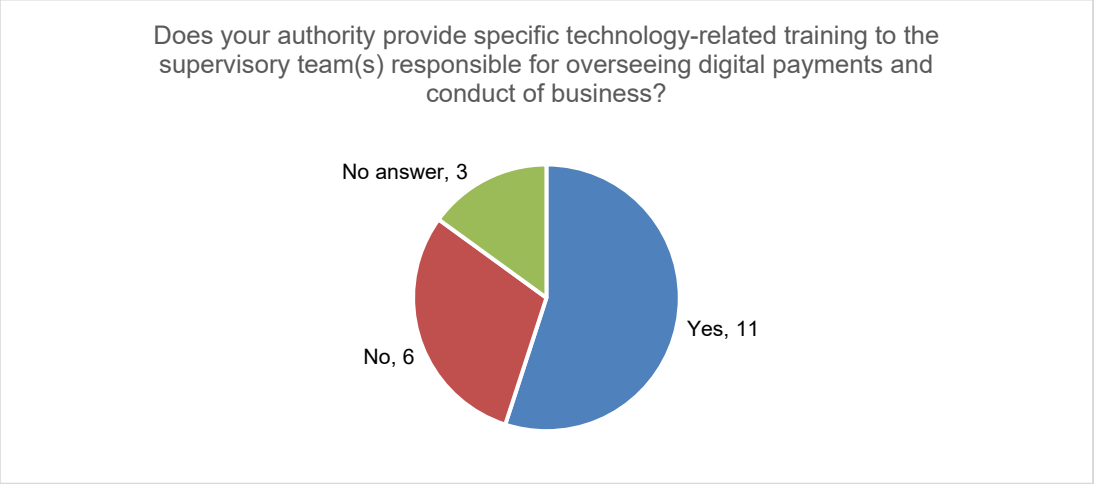
Figure 7. Employment of staff with expertise in digital technologies



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

Keeping pace with technological innovation requires highly skilled and motivated staff, that have access to quality resources and targeted training. The majority of survey respondents reported employing staff with expertise in digital technologies, either in the team responsible for supervising conduct of business or in the team responsible for the oversight of payments (see Figure 7). Notably, three respondents that do not currently employ staff with expertise in digital technologies are considering or planning to hire staff with expertise in areas relevant for supervising digital payments, such as: IT, systemic risks, cyber-security, computing science, data science, data collection and analysis, programming languages, AI, cryptography, digital payments and FinTech.

Figure 8. Technology-related trainings offered to supervisory teams



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

As shown in Figure 8, most responding authorities offer specific technology-related training to the supervisory teams responsible for overseeing digital payments and conduct of business (N=11).

While authorities usually have continuous offers of general training to their supervisory teams, training on specific skills or areas related to market conduct supervision of digital payments is mostly upon solicitation, according to supervisory needs.

Training may either be provided in-house (e.g., by employed experts or by specific departments within the authorities) or not; external training is offered either by private entities or through cooperation with international organisations.

Some of the specific technology-related trainings for overseeing digital payments and conduct of business mentioned by authorities are on data analysis, FinTech, blockchain and information security. Other examples are provided in Box 5.

Box 5. Examples of training initiatives

Training offerings at the Central Bank of **Brazil** include industry courses, in-house courses guided by more experienced staff, corporate university classes, and international cooperation mechanisms.

In **Australia,** ASIC, besides offering its staff external training initiatives, such as industry conferences, also provides wide training sessions in new innovative areas facilitated by its Innovation Hub and internal learning programmes.

The supervisory team at the Bank of **Mauritius** receives training in FinTech, cloud computing, Central Bank Digital Currency, AML/CFT matters and cyber security risks. The Bank also benefits from technical assistance from the International Monetary Fund and the World Bank.

3.6. Consumer awareness initiatives

Regarding consumer awareness initiatives, all responding authorities reported the existence of communication strategies and campaigns to inform consumers about the characteristics and risks of digital payment services. In all cases, the responding authority put in place or contributes to the consumer awareness initiatives.

Nearly all respondents (N=16) publish content regarding security issues related to digital payment services on their websites.

A similarly large share of respondents (N=17) reported that a financial literacy body (or bodies) in their jurisdiction ran initiatives or campaigns to promote responsible security practices by users of digital payments services. Of these respondents, the majority (N=15) specified that the financial literacy body (or bodies) disseminated information on the features and risks of digital payment services based on inputs from financial supervisors.

Finally, in the jurisdictions of 16 respondents, PSPs are required to promote responsible behaviours by digital payment services' users to protect themselves from potential harm.

4. Security incidents, scams and frauds

Keeping a high level of security in digital payments is crucial in order to ensure that users approach them without being afraid of being targeted by fraudsters. This chapter presents trends related to security incidents, scams and frauds, including targeted groups and affected instruments. It further describes monitoring and reporting mechanisms, security tools, disclosure requirements, and coordination and information-sharing practices.

4.1. Trends, targeted groups, affected instruments/mechanisms

Nearly half of respondents (N=9) reported an increase of the number of security incidents linked to digital payments over the last three years; three reported that the number had decreased and another three reported it had remained the same.

The survey asked for specific data on the number of security incidents for the past three years, but most respondents (N=16) were not able to provide the necessary data. This may indicate the need for strengthened data collection in this area. Of the authorities that were able to provide the annual numbers of security incidents for 2018, 2019 and 2020, the reported increases ranged from 30% to 1,446% over the three-year period.

For security incidents, the most commonly affected payment instruments are internet banking, mobile banking, and payment cards. In many cases, security incidents are due to operational issues occurring on card platforms or authentication servers, as well as in clearing and settlement systems – including human errors linked to the upgrading of IT systems or treatment errors (e.g., payment orders submitted twice, erroneous transaction cancellation).

Regarding the number of scams and frauds, the vast majority of respondents (N=17, or 85% of respondents) reported an increased frequency in the last three years. The remaining respondents reported that the information was not available. The survey also asked for specific data on the number of scams and frauds per year for the last three years but—similar to the question about security incidents—most respondents (N=16) were not able to provide the data. Among those that reported annual data from 2018 to 2020, increases ranged from 5% to 508% over the three-year period.

Based on information reported from jurisdictions with available data, frauds and scams affect all consumers, with the most commonly targeted groups being seniors and/or newly retired people, retail investors, and immigrants. The most commonly affected payment instruments are payment cards, internet banking and mobile banking.

4.2. Monitoring and reporting on security incidents or scams and frauds

Security incidents, scams and frauds are among the most relevant threats to consumer protection, particularly regarding digital transactions.

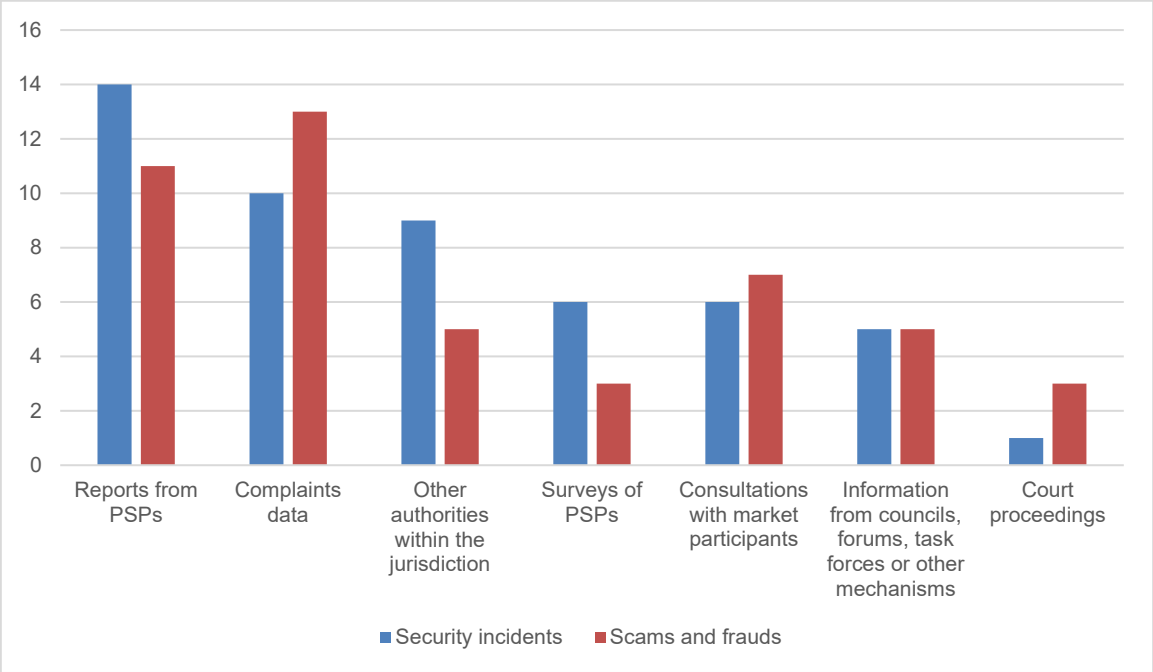
According to survey responses, a significant majority of authorities monitor security incidents (N=17) or scams and frauds (N=16) linked to digital payments. Reporting on security incidents or scams is mandatory for a relevant number of respondents (N=14 for security incidents; N=13 for scams and frauds); however, almost the remaining respondents do not require any mandatory reports on security incidents or on scams and frauds.

EU jurisdictions reported collecting data on these issues under the PSD2. Data is reported to the European Central Bank (ECB) according to the provision of the EBA Guidelines on Fraud Reporting.

PSPs may be required to submit periodic reports on different basis (e.g. weekly, or monthly). Notably, one respondent mentioned that according to the supervisory guidelines, reports would be prescribed in case of a system failure or other reportable events and must describe the damage, the cause of the failure and the status of the action taken.

As shown in Figure 9, among the sources to monitor security incidents or scams and frauds, the most common responses are reports from PSPs and complaints data. Consulting with other authorities at a national level is also common for monitoring security incidents – less so for the purpose of monitoring scams and frauds.

Figure 9. Information sources used to monitor security incidents, scams and frauds



Note: N=20.
Source: FinCoNet Survey on Supervisory Challenges Relating to the Increase in Digital Transactions (2021).

Reporting on frauds may be categorised by different means of payment. When monitoring security incidents or scams and frauds, most authorities reported using the same approach irrespective of the channel used (e.g., POS, online, platforms). In some cases, however, the channel used may affect other aspects of supervisory responses. For example, one respondent reported that, when assessing a complaint concerning an operation executed using a POS device, the PSP may be required to provide the contract, internal records, tickets and other documentation to prove that the disputed operations were properly authenticated and/or executed. Monitoring cyber incidents may include different approaches, such as gathering information from PSPs and collecting information available from different sources (e.g. other authorities, or even the press). The Central Bank of the **United Arab Emirates** on-boards banks to a dedicated information-sharing platform for the purposes of communication and sharing of cyber and financial fraud incidents.

4.3. Tracking new types of security risks

Tracking emerging risks is a challenge for authorities, and many are devising their own approaches to address this need. The majority of respondents reported a specific initiative in place regarding emerging security risks, primarily data collection; other relevant initiatives include public/private sector information sharing platforms, coordination with telco authorities, information sharing mechanisms with foreign regulators and international payment system networks. Emerging risks may also be monitored based on insights from innovation hubs and regulatory sandboxes established to foster technological innovation in the financial services industry.

4.4. Security tools used by digital payments providers

Responding authorities described a range of tools deployed to mitigate security risks linked to digital payments. In some cases, regulated entities are required to implement specific tools; in other cases, supervisory authorities mentioned that each provider would be responsible for identifying the security tools that would better fit their situation. Jurisdictions in the EU, for example, leverage on the PSD2 and the EBA regulations to set regulatory requirements for re-enforcement of security in the digital payment space. A few authorities stated that they allowed payments providers to decide which tools to use. This may include, however, assessing the proposed tools and proposing enhancements where required.

Strong customer authentication, data protection requirements, cyber security risk management and transaction monitoring have emerged as the most common tools adopted to secure the digital payment environment. The responses also demonstrate that tools are often adapted to the evolution of the risks identified.

Certain responding authorities supplement these supply-side initiatives with consumer awareness campaigns and financial education initiatives.

4.5. Disclosure requirements

Although safety issues are at the top of the national and international agenda, regulators are also challenged to address other crucial financial consumer protection topics. In a period of rapid change in consumer habits driven by technological innovation and the persistence of the COVID-19 pandemic, it is of the utmost importance to identify effective approaches to ensure that disclosure of information is appropriate, timely, and helps to guarantee that consumers are aware not only about the digital financial services' benefits, but also their risks.

Supervisory approaches concerning the disclosure of digital payment services' features differ among respondents.

In particular, several jurisdictions developed specific measures to ensure the disclosure of information by PSPs to users of payment services about security risks, scams and frauds or security procedures.

EU jurisdictions follow the harmonised and detailed framework provided for by the PSD2; in the **United Arab Emirates**, these disclosures are part of the licensing regulation.

Some respondents reported that they have no specific disclosure requirements relating to security risks, scams and frauds or security procedures; however, additional disclosure may be mandated under self-regulatory initiatives.

As far as the delivery channel or the technological platform used to perform the transaction is concerned, the majority of respondents reported that disclosure requirements do not differ. Supervisory bodies have generally designed their disclosure requirements having in mind a technologically neutral approach, regardless of the delivery channel used to perform the transaction. Examples of digital-specific guidelines and recommendations are set out in Box 6.

Box 6. Guidelines and recommendations on disclosure and transparency for digital channels

Only a few respondents reported having specific disclosure requirements according to the distribution channel (N=3). In one example, **Bank of Mauritius** reported that the *Guideline on Mobile Banking and Mobile Payments Systems* requires payment service providers to provide instructions to customers on how to configure their mobile devices to access mobile and payment applications and advise customers on necessary security precautions in using mobile banking and payment services. The *Guideline on Internet Banking* stipulates that financial institution should inter alia ensure that they inform customers of the risks involved in the use of Internet Banking services and that customers know their rights and responsibilities with regard to Internet Banking.

The **Banco de Portugal** published a set of general and specific recommendations to promote transparency of information in digital channels and ensure that bank customers have access to complete, appropriate and clear information. The general recommendations state that institutions shall ensure that, for instance: the font size used is sufficient to ensure that information is clearly legible; the colours or images used do not make it difficult for bank customers to read the information provided; the brand used to offer a banking product or service is accompanied by the identification of the institution responsible for the product or service with equal prominence. Specific recommendations are also provided to institutions to be adopted in accordance with the respective stage of the contractual process. Institutions must ensure that, for instance: information on the basic features of the banking product or service and other relevant elements, such as any fees or charges, is displayed in a prominent manner; options have not been selected by default; robust methods are used to ensure that bank customers exercise consent.

4.6. Digital IDs

There are a number of initiatives in place using secure means of identification and authentication to mitigate risks associated with digital financial services.

Half of respondents reported having already implemented a legally recognised and unique digital ID. However, only a minority of respondents reported using digital IDs in the context of payments.

4.7. Transaction limits

Most respondents impose legal or regulatory limits on digital transactions, primarily determined by transaction amounts and transaction type. There is a general trend to set low

value limits on contactless payments without strong customer authentication as the risk associated with payments without customer authentication are higher (in particular, the risk of fraud). Some jurisdictions cap periodical cumulative transaction values and amounts of e-money held in wallets, while others apply limits based on channels; accordingly, wallet transfers are capped at very low values while transfers on the instant payment system, which features strong customer authentications, can increase up to 10 times the cap of mobile payments. In **Japan**, Funds Transfer Service Providers are categorised into three tiers, each with different limits on the maximum value per remittance. In the **United Arab Emirates**, the Central Bank may impose certain limits on digital payments depending on the entity to be licensed.

Around a third of respondents do not impose transaction limits, leaving PSPs to set their own limits; however, some respondents mentioned that limits may arise from AML legislation.

4.8. Sharing information and coordinating internationally

A majority of respondents exchange information about security incidents, scams and frauds with foreign financial supervisory authorities or with international organisations.

The ECB and EBA were mentioned by most EU member states when sharing information regarding security incidents, scams and frauds. Respondents also mentioned other supervisory authorities for the exchange of information where they deemed it necessary. Furthermore, the respondents mentioned international fora like FinCoNet for information exchange.

Most respondents reported taking action when confronted with an indication that a PSP of their jurisdiction was causing harm for payment service users in other jurisdictions. The approach varied based on the applicable regulatory framework (e.g. within the EU, a passporting regime exists according to which supervisory actions are generally under the remit of the "home country" of the PSP – i.e., the jurisdiction where it was authorised). Some respondents reported not being able to take any actions when a user outside of their jurisdiction runs into a dispute with a PSP from the authorities' jurisdiction.

Conversely, when a user of payment services of the respondent authorities' jurisdiction suffers a loss or is defrauded by a PSP authorised in another jurisdiction, respondents reported that they would not have the authority or legal powers to take action. Within the EU, the passporting regime mentioned above allows for PSPs authorised in one member state to provide services throughout the EU, while remaining subject to the supervision of their home authority. The supervisory authority of the host member state, however, retains some powers in order to address the most critical cases – e.g., in order to avoid that the infringements by the PSP result in the detriment of payment users.

5. Key findings and next steps

The following key findings emerge from this Report:

- Governance, frameworks and challenges
    - At least one authority in each jurisdiction is responsible for the regulation and supervision of payments. In most cases, this is carried out by a single authority (such as a central bank). Cooperation mechanisms among different authorities regarding digital payments are fairly common, even in jurisdictions where the responsibility is not shared.
    - Banks and payment institutions are the most common types of payment providers subject to market conduct regulation. Telco providers and platforms are less commonly subject to market conduct regulations.
    - The supervision of digital payments presents four key challenges: vulnerability to cyber risks; vulnerability to frauds and scams; need to adapt regulation and supervisory practices; and lack of awareness among consumers.
- Market conduct supervision tools & consumer awareness initiatives
    - Authorities take a range of approaches toward market conduct supervision of digital payment services. Two models were identified: risk-based classification of providers and defined standards. In some cases, market conduct requirements differ according to payment channels; in other cases, the same requirements apply irrespective of the channel (digital or non-digital).
    - Regarding supervisory tools, on-site inspections, off-site inspections and analysis of complaints data were deemed some of the most effective tools to detect misconduct in the field of digital payments. The COVID-19 pandemic has elevated the urgency of implementing remote supervisory activities, often using SupTech tools.
    - Regarding corrective actions taken when misconduct has been detected, sending supervisory letters and issuing guidelines were ranked among the most effective.
    - The employment of staff with expertise in digital technologies by authorities is now common, as well as the provision of specific technology-related trainings to the supervisory teams responsible for overseeing digital payments and conduct of business.
    - Authorities have communication strategies and campaigns to inform consumers about the characteristics and risks of digital payment services.
- Security incidents, scams and frauds
    - In the last three years, the number of security incidents, scams and frauds linked to digital payments have increased in most jurisdictions.

- The most commonly affected instruments/mechanisms by security incidents and scams and frauds are internet banking, mobile banking and payment cards.
- The consumer groups most commonly affected by frauds and scams are seniors and/or newly retired people, retail investors, and immigrants.
- The most common sources used to monitor security incidents or scams and frauds are reports from PSPs and complaints data. Consulting with other authorities at a national level is also common for monitoring security incidents – less so for the purpose of monitoring scams and frauds.
- Authorities have in place specific initiatives to track emerging security risks, such as data collection, public/private sector information sharing platforms, coordination with telco authorities, information sharing mechanisms with foreign regulators and international payment system networks. Emerging risks may also be monitored based on insights from innovation hubs and regulatory sandboxes established to foster technological innovation in the financial services industry.
- Authorities reinforce the importance of ongoing and comprehensive monitoring of security incidents, scams and frauds linked to digital payments, highlighting that reporting requirements for regulated entities are one of the most relevant information sources used to monitor these trends. Moreover, authorities emphasise the relevance and utility of exchanging information about security incidents, scams and frauds with foreign financial supervisory authorities or with international organisations (such as FinCoNet).

Looking ahead

The role of digital payments in consumer finance is growing fast. Market conduct supervisors need to be prepared to monitor new payment products and services, business models and providers, in order to stay abreast of the conduct risks, ensuring an adequate conduct supervision and consumer protection. This task may pose challenges, particularly for authorities in jurisdictions with significant resource constraints. At the same time, heightened adoption of SupTech tools could address these constraints by automating and accelerating certain processes.

Next steps

Building on this initial stocktaking exercise, a set of interesting and topical issues emerge, one or more of which could form the basis of a follow-up report from FinCoNet. Namely, the report may reflect on the implications of BigTech companies offering digital payment services, consider the role of non-financial entities such as telco providers and platforms, dive deeper on the extent to which the regulatory and supervisory framework addresses security standards for payments (including the misuse and abuse of consumer data), develop case studies on specific supervisory challenges or gather best practices on data reporting.

References

European Commission (2015), "Payment services (PSD2) – Directive (EU) 2015/2366", European Commission, https://ec.europa.eu/info/law/payment-services-psd-2-directive-eu-2015-2366_en.

FinCoNet (2016), "Online and mobile payments: Supervisory challenges to mitigate security risks", FinCoNet, http://www.finconet.org/FinCoNet_Report_Online_Mobile_Payments.pdf.

FinCoNet (2018), "Online and mobile payments: An overview of supervisory practices to mitigate security risks", FinCoNet, http://www.finconet.org/FinCoNet_SC3_Report_Online_Mobile_Payments_Supervisory_Practices_Security_Risks.pdf.

Appendices

Appendix A: List of responding authorities

Jurisdiction	Responding authority
Australia	Australian Securities and Investments Commission
Brazil	Banco Central do Brasil
Canada	Financial Consumer Agency of Canada (FCAC)
France	Autorité de Contrôle Prudentiel et de Résolution (ACPR)
Germany	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)
Indonesia	Otoritas Jasa Keuangan
Indonesia	Bank Indonesia
Ireland	Central Bank of Ireland
Italy	Bank of Italy – Banca d'Italia
Japan	Japan Financial Services Agency (JFSA)
Republic of Mauritius	Bank of Mauritius
Mozambique	Banco de Moçambique
The Netherlands	The Dutch Authority for the Financial Markets (AFM)
Peru	Superintendence of Banking, Insurance and Private Pension Fund Administrators (SBS)
Portugal	Central Bank of Portugal ("Banco de Portugal")
Russian Federation	Bank of Russia
South Africa	South African Reserve Bank
Spain	Banco de España
United Arab Emirates	Central Bank of the UAE

Appendix B: Questionnaire

Section A. Governance

1. *In your jurisdiction, which authority/ies is/are responsible for the regulation and supervision of payments, including digital payments? Please select all that apply.*

☐ Market conduct supervisor
☐ Prudential supervisor
☐ Payments systems overseer/authority
☐ Other single authority (e.g., Central Bank)
☐ Other – please specify:

2. *Please provide information about any inter-agency forums, task forces, councils or other mechanisms for different regulators and authorities to exchange information and coordinate activities related to the following topics, if any are in place in your jurisdiction.*

	Payments	*Digital financial services*	*Cross-border issues*
Is a mechanism in place to coordinate work on this topic? (Yes/No)			
What is the structure (e.g., MoU or other formal relationship)?			
What is the mandate of the body?			
Which authorities participate?			
Does it meet or exchange information on a regular basis?			
What kinds of information are exchanged?			

3. *If applicable, please provide examples of recent initiatives in the field of digital payments carried out by the body(ies) mentioned above.*

Section B. Legal and regulatory framework for digital payments

4. *Does your authority have a specific mandate to supervise the market conduct of digital payment services providers?*

☐Yes

☐No

4.1. *If yes, please specify in which legislation, rules or guidance such mandate is established. If no, please indicate which authority, if any, is entrusted with this task in your jurisdiction.*

5. *If yes, which of the following powers or functions does the mandate include? Please select all that apply.*

☐	Granting (or refusing to grant) the authorisation to provide digital payment services
☐	Control over qualifying holdings
☐	Exercising regulatory powers
☐	Approving and reviewing the contractual terms and user agreements for digital payment services or channels
☐	Overseeing the internal controls and organisational procedures to be implemented by digital payment services providers
☐	Limiting the remuneration of management and of financial agents providing digital payment services
☐	Receiving and replying to complaints from users of digital payments
☐	Limiting the applicable fees and general costs of digital payment services. Please specify whether price caps apply:
☐	-To the fees applicable to the consumers as a payer;
☐	-To the fees applicable to the merchant by the acquirer payment services providers (PSP)
☐	-To the fees levied between or among the payment services providers
☐	Assessing the digital payment services providers' business on the basis of a risk-based approach
☐	Collecting information and statistics concerning digital payments
☐	Issuing warnings to providers of digital payments services
☐	Adopting binding decisions vis-à-vis the digital payment services providers
☐	Applying pecuniary (or non-pecuniary) sanctions vis-à-vis the digital payment services providers
☐	Promoting policy and regulatory changes whenever required
☐	Coordinating with other regulators, domestic and cross-border, for supervision of payment service providers and other entities directly or indirectly involved in payment services
☐	Other - please indicate:

6. Which types of providers of digital payments services are subject to laws, regulations, and guidance relating to market conduct and financial consumer protection in your jurisdiction? Please select all that apply.

☐	Banks
☐	Payment institutions
☐	E-money institutions
☐	Platforms
☐	Payment aggregators
☐	Open banking services (e.g., account information service providers)
☐	Telco providers
☐	Others – please specify:

6.1. Please provide any additional information, including whether any of the provider types ticked above are subject to additional financial consumer protection laws, regulation or guidance that are specific to that type of provider.

7. In your jurisdiction, to which types of users do the laws, regulation or guidance regarding digital payment services apply? Please select all that apply.

☐	Consumers
☐	Individual entrepreneurs
☐	Small businesses
☐	All businesses, regardless of their size
☐	Other – please specify:

8. What are the primary challenges currently facing market conduct supervisors relating to digital payments? ***Please select up to five (5).***

☐	Digital payments are mostly offered by unregulated/unsupervised entities
☐	Consumers lack awareness of risks related to digital payments
☐	Digital payments are more vulnerable to frauds and scams
☐	Digital payments are more vulnerable to cyber risks
☐	It is challenging to coordinate with other relevant entities/authorities who have shared or overlapping oversight responsibilities
☐	Authorities require stronger IT skills and systems

☐	Data on digital payments is not available
☐	Regulation and supervisory approaches need to adapt
☐	Enforcement tools are not available or authorised
☐	New entrants are unfamiliar with laws, regulation and guidance governing digital payments
☐	It is not possible to keep up with technological and market developments
☐	Other – please elaborate:

9. *Which approaches are most effective for supervisors and regulators to stay abreast of technological and market developments while overseeing the evolution of the sector and managing new market conduct risks linked to the growth of digital payments?* ***Please select up to five (5).***

☐	Regular consultation with market participants, including industry bodies and consumer groups
☐	Setting up an innovation hub/regulatory sandbox
☐	Mandatory reports of PSPs
☐	Surveys of PSPs
☐	Surveys of digital payment services' users
☐	Introducing innovative monitoring tools
☐	Exchange of information among national supervisory authorities (financial and non-financial sector)
☐	Participation in international groups and initiatives related to digital payments
☐	Analysis of complaints data
☐	Exchange of information with supervisory authorities from different jurisdictions
☐	Other – please specify:

10. *Does your jurisdiction have rules or regulations allowing digital payments services to be provided to consumers by a third-party entity on behalf of the payment service provider (e.g., agents, correspondents, cash-in/out outlets, etc.)?*

☐ Yes

☐ No

10.1. *Please explain your answer above.*

11. *Does your jurisdiction have rules or regulations allowing digital payments services to be initiated by the consumer through a third-party entity, not on behalf of the payment service provider (e.g., payment initiation services providers, open banking mechanisms)?*

☐ Yes

☐ No

11.1. Please explain your answer above.

Section C. Security incidents, scams and frauds

12. In your jurisdiction, how has the number of security incidents, scams and frauds linked to digital payments changed in the last 3 years?

	Increased	Decreased	Stayed the same	Information not available
Number of security incidents	☐	☐	☐	☐
Number of scams and frauds	☐	☐	☐	☐

13. Please indicate the number of security incidents, scams and frauds linked to digital payments reported each year for the last 3 years. Enter N/A if the information is not available.

	2018	2019	2020
Number of security incidents			
Number of scams and frauds			

14. Please indicate which of the following segments of consumers are more frequently the target of scams and frauds through digital payments in your jurisdiction. Please select all that apply.

☐ All consumers (i.e., no particular group is targeted)

☐ Seniors and/or newly retired people

☐ Youth

☐ Men

☐ Women

☐ Retail investors

☐ Immigrants

☐ Members or veterans of the military

☐ Information not available

☐ Other – please specify:

15. Which digital payment instruments, technologies or mechanisms are most frequently affected by security incidents or scams and frauds in your jurisdiction? ***Please select up to five (5) for each column.***

	Security incidents	Scams and frauds	Information not available
Contactless payments	☐	☐	☐
Payment cards	☐	☐	☐
Pre-paid cards	☐	☐	☐
Mobile banking	☐	☐	☐
Mobile point of sales (mPOS)	☐	☐	☐
Social media payment options	☐	☐	☐
Mobile wallets	☐	☐	☐
Internet banking	☐	☐	☐
Other – please specify:	☐	☐	☐

15.1. Please provide any additional information on your answers above.

16. Does your authority monitor security incidents or scams and frauds linked to digital payments?

	Yes	No
Security incidents	☐	☐
Scams and frauds	☐	☐

17. Does your authority require mandatory reports on security incidents or scams and frauds from PSPs?

	Yes	No
Security incidents	☐	☐
Scams and frauds	☐	☐

17.1. If your authority requires mandatory reports on security incidents or scams and frauds, please provide any additional details.

18. If applicable, please identify which sources your authority uses to monitor security incidents or scams and frauds. Please select all that apply.

	Security incidents	Scams and frauds
Reports from PSPs	☐	☐
Surveys of payment services providers	☐	☐
Court proceedings	☐	☐
Other authorities within your jurisdiction (from financial and non-financial sectors)	☐	☐
Complaints data	☐	☐
Consultations with market participants	☐	☐
Information from National Payments Council, inter-agency forum, task force, or other mechanism	☐	☐
Other – please explain:	☐	☐

19. When monitoring security incidents or scams and frauds, does your authority have a specific approach depending on the channel used (POS/online/platforms/etc.)?

	Yes	No
Security incidents	☐	☐
Scams and frauds	☐	☐

19.1. Please provide any additional details.

20. How does your authority track new types of security risks? In particular, does your authority have a specific initiative regarding emerging security risks? Please describe.

21. What are the main security tools and mechanisms adopted by providers of digital payments? Please describe.

22. Does your authority supervise the disclosure of digital payment services' features?

☐ Yes

☐ No

23. Has your authority developed specific measures to ensure the disclosure of information by PSPs to users of payment services about security risks, scams and frauds or security procedures?

	Yes	No
Security risks	☐	☐
Scams and frauds	☐	☐
Security procedures	☐	☐

23.1. Please provide any additional comments on your answers above.

24. Do the disclosure requirements differ according to the delivery channel or the technological platform used to perform the transaction?

☐ Yes

☐ No

24.1. Please explain your answer above.

25. Does your jurisdiction have in place a legally recognised and unique digital ID system that authenticates personal identity and ensures its uniqueness?

☐ Yes

☐ No

26. If yes, is the digital ID System used in the context of digital payments?

☐ Yes

☐ No

27. Are transaction limits—either legal or regulatory—imposed on the use of digital payments in your jurisdiction? Please describe.

28. Does your authority exchange information regarding security incidents or scams and frauds with foreign financial supervisory authorities or with international organisations?

	Yes	No
Security incidents	☐	☐
Scams and frauds	☐	☐

28.1. Please provide any additional details on your answers above.

29. If a payment service user in another jurisdiction suffered a loss or was defrauded/scammed through a cross-border payment service provided by a PSP authorised in your jurisdiction, could your authority take administrative actions (i.e., enforcement) or apply other penalties against the PSP in your jurisdiction? If yes, please provide additional details, including the possible administrative actions or penalties.

30. 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, would your authority have supervisory procedures/powers to act? If yes, please identify what kind of supervisory actions or operations would be possible.

Section D. Market Conduct Supervision Tools & Consumer Awareness Interventions

31. *Does your authority have in place a specific risk-based approach to market conduct supervision of digital payments services?*

☐ Yes

☐ No

31.1. *If Yes, please explain:*

32. *Does your authority have a specific approach to market conduct supervision depending on the digital payment channel used?*

☐ Yes

☐ No

32.1. *If Yes, please explain:*

33. *Please select the appropriate responses regarding SupTech tools that your authority has implemented or is planning to implement to a) monitor risks to consumers stemming from the use of digital payments or b) prevent or mitigate those risks.*

	Already implemented	Not implemented yet, but planning to implement	Not implemented and not planning to implement
a) SupTech tools to **monitor** risks to consumers stemming from digital payments	☐	☐	☐
b) SupTech tools to **prevent or mitigate** risks stemming from digital payments	☐	☐	☐

33.1. *Please provide additional details about any SupTech tools relating to digital payments that your authority has implemented or is planning to implement.*

34. Does your authority monitor PSPs' websites, online platforms, apps, and other digital channels to assess a) their compliance with mandatory requirements on the disclosure of security risks and b) their implementation of required precautionary measures to prevent fraud, scams and security incidents?

a) *b)*

35. In your supervisory capacity, which supervisory tools do you deem to be the most effective to detect misconduct in the field of digital payments? ***Please select up to five (5).***

☐	Desk-based reviews
☐	On-site inspections
☐	Reporting requirements of PSPs
☐	Off-site inspections
☐	Mystery surfing/mystery shopping
☐	Meetings with supervised entities
☐	Analysis of complaints data
☐	Monitoring of advertisements
☐	Other – please specify:

35.1. Please provide additional details on any of the tools ticked above.

36. In your supervisory capacity, which corrective actions do you deem to be most effective to address misconduct in the field of digital payments? ***Please select up to three (3).***

☐	Issuing guidelines addressed to all market participants
☐	Sending supervisory letters to supervised entities that infringed the applicable regulation
☐	Applying administrative fines
☐	Licence withdrawal
☐	Banning the supervised entity from entering into further contracts with consumers
☐	Other – please specify:

36.1. Please provide additional details on any of the actions ticked above.

37. Does your authority employ staff with expertise in digital technologies?

☐ Yes, in the team responsible for supervising conduct of business

☐ Yes, in the team responsible for the oversight of payments

☐ No, but we are hiring or planning to hire staff with expertise in digital technologies to work in the conduct of business supervision or the oversight of payments

☐ No, and we do not have plans to hire staff with these skills

37.1. Please specify the areas of expertise, if applicable.

38. Does your authority provide specific technology-related training to the supervisory team(s) responsible for overseeing digital payments and conduct of business?

☐ Yes

☐ No

38.1. Please provide additional information on the trainings.

39. In your jurisdiction are there communication strategies and campaigns to inform consumers about the characteristics and risks of digital payment services?

☐ Yes

☐ No

40. Does your authority put in place or contribute to communication strategies and campaigns to make consumers aware of the characteristics and risks of digital payment services?

☐ Yes

☐ No

41. Does your authority publish content regarding security issues related to digital payment services on its website?

☐ Yes

☐ No

42. If your jurisdiction has in place a financial literacy body, 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?

☐ Yes

☐ No

43. Does the financial literacy body (or bodies) run initiatives or campaigns to promote responsible security practices by users of digital payments services?

☐ Yes

☐ No

44. Are PSPs required to promote responsible behaviours by users of digital payments services to protect themselves from potential harm?

☐ Yes

☐ No

45. You have reached the end of the survey. Please use the space below to provide any additional information not yet addressed.


FinCoNet
INTERNATIONAL FINANCIAL CONSUMER
PROTECTION ORGANISATION