FIGI
FINANCIAL INCLUSION GLOBAL INITIATIVE

Legal Framework for Cybersecurity in the Financial Sector

A Comparative Study on Existing Domestic or Regional Legislation on Cybersecurity

FEBRUARY 2022

WORLD BANK GROUP

ACKNOWLEDGMENTS

This paper was prepared by Professor Maria Chiara Malaguti, Dorothee Delort and Carol Lee (World Bank Group, Finance, Competitiveness and Innovation Global Practice), with the assistance of Ludovica Gabrielli and Renuka Pai, under the guidance of and the leadership of Mahesh Uttamchandani and Harish Natarajan (World Bank Group, Finance, Competitiveness and Innovation Global Practice), in the context of the Financial Inclusion Global Initiative Working Group on cybersecurity (under the Security and Trust Working Group). The authors thank Fredes Montes (World Bank Group, Finance, Competitiveness and Innovation Global Practice) and Emran Islam (International Monetary Fund) for their review of the paper and their input.

The interpretations and conclusions expressed in this work belong to the authors and do not necessarily reflect the views or positions of either the World Bank Group, its Board of Executive Directors, and the governments they represent, or the Bill & Melinda Gates Foundation.

FINANCE, COMPETITIVENESS & INNOVATION GLOBAL PRACTICE
Payment Systems Development Group

1818 H Street NW, Washington, DC 20433
Telephone: 202-473-1000; Internet: www.worldbankgroup.org

DISCLAIMER

The Financial Inclusion Global Initiative led in partnership by the World Bank Group (WBG), International Telecommunication Union (ITU), and the Committee on Payments and Market Infrastructures (CPMI), with the support of Bill & Melinda Gates Foundation (BMGF). The FIGI program is a three-year investment funding national implementations in three countries (China, Egypt, and Mexico), supporting topical working groups to tackle 3 sets of outstanding challenges in closing the global financial inclusion gap, and hosting 3 annual symposia to gather the engaged public on topics relevant to the grant and share intermediary learnings from its efforts.

This work has been prepared for the Financial Inclusion Global Initiative by the Cybersecurity for FMI's Workstream of the FIGI Security, Infrastructure and Trust (SIT) Working Group. The work is a product of the staff of the World Bank with external contributions prepared for the Financial Inclusion Global Initiative. The findings, interpretations, and conclusions expressed in this work do not necessarily reflect the views of the Financial Inclusion Global Initiative partners partners including The World Bank, its Board of Executive Directors, or the governments they represent, or the views of the Committee for Market Payments Infrastructure, International Telecommunications Union, or the Bill & Melinda Gates Foundation. The World Bank does not guarantee the accuracy of the data included in this work. The boundaries, colors, denominations, and other information shown on any map in this work do not imply any judgment on the part of The World Bank concerning the legal status of any territory or the endorsement or acceptance of such boundaries.

Table of Contents

Acronyms and Abbreviations

APRA	Australian Prudential Regulation Authority
CII	critical information infrastructure
CSA	Cyber Security Agency (Singapore)
CSIRT	computer security incident-response teams
DFS	Department of Financial Services (New York)
EBA	European Banking Authority
ECB	European Central Bank
EFT	electronic fund transfer
ENISA	European Union Agency for Cybersecurity (European Network and Information Security Agency)
ESA	European Supervisory Authorities
ICT	information and communications technology
NIS	network and information systems
PSD	Payment Service Directive

Executive Summary

In this time of digital transformation, cybersecurity is more essential than ever. However, cybersecurity is still a blurred concept to many extents. The growing prevalence and cost of cyberattacks are key challenges for the financial sector. Even though cybersecurity has recently become a hot topic, there is still no common definition of this term. The definitions provided in this paper (which represent only a sample of the many that can be found in policy and legal texts) refer to general measures to reduce cyber risk and information and communications technology (ICT) risk and to ensure protection. They broadly include, but do not directly refer to, provisions of criminal law to punish those committing cybercrimes.

From a comparative analysis of legal systems in different regions or countries, it appears that cybersecurity issues are mainly addressed through two different approaches: (i) systems that adopted a fully fledged cybersecurity law (that is, China, Nigeria, and Singapore) and established an authority in charge of its implementation (although with differences in competence and tools); and (ii) systems where no cybersecurity law has been adopted at this stage (that is, the United States) but other statutory acts, covering a specific matter, also cover issues relevant for cybersecurity, such as authorization of orders or transactions, and fraud. In the alternative, regulators cover some aspects of cybersecurity within the scope of their mandate (that is, the European Supervisory Authorities for the financial market on the one side and the European Central Bank on the other), thus addressing relevant issues but limited to supervised/overseen entities.

Since cybersecurity risk in fact requires articulated tools to ensure satisfactory protection, the two above approaches might coexist. Even when a cybersecurity law is adopted, a few issues are usually left out and regulated by other means or by institutions other than the cybersecurity authority. Often existing authorities deal with ICT/cybersecurity risk management within their respective competences and establish standards to make more resilient operators and networks that implement existing cybersecurity legislation.

Different approaches affect how cybersecurity in the financial sector is regulated. Indeed, lacking an overarching law on cybersecurity, the financial regulator might establish secondary measures based on existing financial legislation to cover cybersecurity specifically by exclusively relying on its authority and thus covering only supervised entities. This ensures consistency of such measures with general regulation of the sector, but its inherently limited scope might impede the authority from covering all required areas of intervention or adopting all relevant instruments. On its side, a general law on cybersecurity might not contain specific provisions for the financial sector and thus risk departing from the logic underlying regulation and oversight of the field. However, it has a far-reaching scope and simultaneously covers financial and nonfinancial entities involved in the provision of financial services (such as IT companies and networks) and can establish tailor-made obligations and actions for mitigating risks.

It thus appears that, irrespective of whether a country adopts legislation on one area or the other, it is difficult to expect that a single piece of legislation could cover all relevant aspects of cybersecurity, when financial markets are concerned. Cybersecurity risk needs to be addressed consistently with all other risks to which the financial markets are exposed. In particular, cybersecurity risk needs to be addressed together with ICT and operational risk. Moreover, issues such as authorization of orders and/or transactions, data protection, and general management of a system or scheme—which do not address only cybersecurity—are already embedded in many separate pieces of legislation. It appears that, even in the presence of a fully fledged cybersecurity law and a cybersecurity authority, the financial regulator still bears a role to implement relevant principles and rules consistently with regulation of financial markets. This would require strengthening of cooperation at both the national and the international level between cybersecurity and financial authorities To that end, international standards may play a relevant role in ensuring consistency and shared solutions.

Introduction

The financial ecosystem is undergoing various changes caused mainly by new technologies and, in particular, digitalization. In this time of transformation, when an incident could easily undermine trust and derail innovation, cybersecurity is more essential than ever. The growing prevalence and cost of cyberattacks are key challenges for financial institutions. Malicious cyber activities (such as ransomware, phishing and spoofing, identity theft, and business email compromise scams) cause disruption and financial loss and even present a significant risk to individuals' rights and freedoms. These risks affect the cyberspace in general, but they represent a specific threat for the financial markets in light of the fiduciary relationship that a customer enters into with the financial intermediary and the need for the public to trust the whole financial system to function smoothly and reach the expected goals of efficiency and inclusion.

There is no common definition of cybersecurity: Although the general area covered is that of protection against crimes within the cyberspace, different definitions highlight different emerging risks and different purposes for measures to mitigate them. Indeed, to compare existing legal frameworks for cybersecurity consistently, and to consider the best choices for mitigation of risk, either in general or specifically for the financial sector, the first issue to address is defining the term and, consequently, the scope of any relevant piece of regulation, as for facts and risks to be covered, interests and entities to be protected, and objectives justifying policy choices in the field. Among the many, in the United States, the Cybersecurity and Infrastructure Security Agency identifies cybersecurity as "*the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information.*"[1] The United Kingdom's National Cyber Security Centre synthetically identifies cybersecurity as the protection of devices, services, and networks, and the information on them, from theft or damage.[2] In the European Union (EU), Regulation 2019/881, known as the Cybersecurity Act, defines cybersecurity as the ensemble of "*the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats.*"[3] Cyber threats, in turn, are broadly defined as any potential circumstance, event, or action that could damage, disrupt, or otherwise adversely affect network and information systems, the users of such systems, and other people. However, the previously adopted Directive 2016/1148, the Network and Information Systems (NIS) Directive, does not use these definitions. It covers obligations to manage risks posed to "*the security of network and information systems*" and focuses mainly on the capability of systems to be resilient. To that end, management of risk is defined as "*the*

BOX 1

COMMON CYBER RISKS

Business email compromise scams exploit the fact that so many of us rely on email to conduct business—both personal and professional—and they are some of the most financially damaging online crimes.

Identity theft happens when someone steals your personal information, such as your Social Security number, and uses it to commit theft or fraud.

Ransomware is a type of malicious software, or malware, that prevents you from accessing your computer files, systems, or networks and demands that you pay a ransom to restore access.

Spoofing and phishing are schemes aimed at tricking you into providing sensitive information to scammers.

Source: FBI, "The Cyber Threat" (web page), **https://www.fbi.gov/investigate/cyber.**

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."[4]

Definitions of cybersecurity are mainly linked to resilience. Although actions against cybersecurity often amount to a crime, and criminal law plays a relevant role as a deterrent against violation, definitions of cybersecurity do not directly refer to punishment of those committing cybercrimes, but to measures to reduce risk and ensure protection. In fact, many criminal codes include a list of "offences against computer security" or the like that includes various cybercrimes, such as hacking, denial-of-service attacks, phishing, and infection of IT systems with computer viruses, which are relevant only as for criminal punishment of specific behaviors. The seriousness of the sanctions imposed under criminal law has an impact on the general policies for mitigating risk, but only indirectly. Measures to mitigate risk and protect relevant stakeholders have their own logics somehow independent and irrespective of the qualification of each individual criminal behavior under criminal law. Criminal acts are relevant insofar as they translate into risks for the ecosystem.[5]

At the international level, international organizations and bodies have attempted some general understanding of the matter by also providing a general definition of cybersecurity. According to the International Telecommunication Union, cybersecurity is "*the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment.*"[6] The general security objectives, comprising availability, integrity (which may include authenticity and nonrepudiation), and confidentiality, are also shared by the Financial Stability Board's Cyber Lexicon, which defines cybersecurity as the preservation of confidentiality, integrity, and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.[7,8]

In line with the Financial Stability Board's definition, risk management usually focuses on what would result if any element of the CIA triad (confidentiality, integrity, and availability) were compromised. In practice, information security is often described in terms of a triad of the elements. When any element of the CIA triad is compromised, the system is considered insecure. Thus, risk management focuses on assessing and reducing the risk to these three critical performance factors.[9] In the absence of a shared definition of cybersecurity and cyberattack, which also implies a lack of shared understanding of the entities that should comply with cybersecurity standards and the values and interests to be protected, the following analysis will broadly refer to the aims identified by the Financial Stability Board's Cyber

Lexicon to cover the spectrum of domestic legislation addressing vulnerabilities, however different their scope might be from country to country.

The Budapest Convention is a cornerstone of cybersecurity at the international level but is not meant to address systematically the mitigation of cyber risk. Rather, it focuses mainly on the protection of users' fundamental rights. The Council of Europe Convention on Cybercrime (2001), known as the Budapest Convention, entered into force in 2004.[10] This is the first treaty on crimes committed through the internet and the like but deals particularly with infringements of copyright, child pornography, and the protection of some fundamental rights, although it also contains provisions on computer-related fraud and violations of network security, and the criminal offenses covered are intended to protect the CIA triad in computer systems or data. It is supplemented by a protocol on acts of xenophobia and racism committed through computer systems. It also contains a series of powers and procedures, such as the search of computer networks and interception. Measures to be taken at the national level by states ratifying the convention include substantive criminal law, procedural law, and jurisdiction.

On the other side, in the financial sector, international standard-setting bodies have given guidance on cyber resilience in specific areas. International standards and recommendations are instruments of soft law but are usually directly implemented by domestic authorities or used as a benchmark, thus affecting domestic governance of financial markets. International standard-setting bodies help domestic authorities to act consistently and follow common paths of action. This occurs mainly through soft-law instruments, which are directly implemented by domestic authorities within their competence and according to the legal order to which they pertain or may work as a benchmark for policy choices under a process of *moral suasion*. In particular, in 2016 the Committee on Payments and Market Infrastructures (CPMI) and the board of the International Organization of Securities Commissions (IOSCO) jointly adopted the *Guidance on Cyber Resilience for Financial Market Infrastructures*, in which they outlined five primary risk-management categories (governance, identification, protection, detection, and response and recovery) and three overarching components (testing, situational awareness, and learning and evolving) that financial market infrastructures should address to ensure cyber resilience. Among implementation measures of such guidance, the 2018 *Cyber Resilience Oversight Expectations for Financial Market Infrastructures* of the European Central Bank (ECB) can be mentioned. These instruments of soft law thus also affect the governance of financial markets to the extent of mitigating cybersecurity risk. The CPMI-IOSCO guidance also strongly encourage collaboration: Because the cyber resilience of financial market infrastructures supports broader financial-stability objectives, and in light of significant interdependencies in clearing and settlement processes, it is important for authorities to cooperate, recognizing that such cooperation may help authorities consider, where appropriate, consistency of direction in their oversight and supervision of both financial market infrastructures and their relevant stakeholders.

From a comparative analysis of legal systems in different regions or countries, it appears that cybersecurity issues are broadly addressed through two different approaches. Although regulation of cybersecurity depends on the specifics of the country's legal order, two approaches can be identified: (i) countries/regions that have adopted a fully fledged cybersecurity law; and (ii) countries/regions where either legislation on a specific matter (such as electronic transactions or e-signatures) also addresses risks caused by, or linked to, cybersecurity acts (for instance, through rules on authorization and fraud), or regulators cover some aspects of cybersecurity within the scope of their traditional mandate.

Different approaches affect how cybersecurity in the financial sector is regulated. In the absence of a cybersecurity law, the financial regulator might still establish specific secondary measures to cover cybersecurity under existing legislation by relying exclusively on its authority. However, when it does so, it can cover only supervised entities (entities under its competence). In turn, a general law on cybersecurity will expand the scope of regulation beyond existing competences but might not contain specific provisions for the financial sector and thus risk departing from the logic underlying oversight of the field. Either choice presents advantages and shortcomings that need to be evaluated according to the circumstances.

Different alternatives can also be combined. When a cybersecurity law exists, rules on the mitigation of risk can often be found in other pieces of legislation, so that the two approaches may in fact overlap and be combined into an articulated legal and regulatory framework. Moreover, a general law on cybersecurity might be implemented in the financial sector by way of secondary measures. In that latter case, the financial authority will keep its scope of regulation and solely address regulated entities but will do so by simultaneously implementing existing financial legislation and the cybersecurity law. That would permit financial authorities to maintain their oversight policy approach but within a wider framework addressing cybersecurity.

In the financial sector, the role of international standards also needs to be assessed as a governance tool to be combined with domestic legislation. Irrespective of the existence of legislation on cybersecurity or even other domestic laws covering some aspects thereof, financial regulators can count upon the results of international cooperation. Standard-setting bodies adopt various recommendations and standards that help domestic authorities to identify relevant issues and common solutions. Although these are soft-law instruments, they are usually transposed directly by domestic regulators into binding internal measures or used as benchmarks for policy choices. Also, when they are not, they might serve as an instrument of moral suasion.

The following study attempts to describe such alternatives and combination thereof by relying on existing legislation in selected countries, and it draws some guidance from lessons learned.

I. Comparative Analysis of Some Domestic Approaches

1. FULLY FLEDGED LAW ON CYBERSECURITY

A still-limited number of countries have adopted specific laws on cybersecurity. For most countries, these laws establish not only a new authority and mechanisms to monitor cybersecurity but also, in some cases, a mechanism to designate critical infrastructures/entities and licensing procedures for entities providing cybersecurity services in the market. However, these laws do not supersede provisions contained in other laws, such as laws on financial services or data protection. Leaving aside domestic legislation on criminal sanctions for cybercrimes—as in the case of one of the first cybersecurity acts ever adopted, the Philippines Cyber Act of 2012,[11] which establishes measures to prevent crimes but, as a whole, focuses on sanctions against cyber offenses—a new generation of cybersecurity acts seem to emerge where an articulated system of regulation and monitoring is established beyond criminal sanctioning and involves new administrative entities, new tasks, and even, in some cases, new (cybersecurity) activities. With no intention to be exhaustive, two parallel models will be discussed in the paragraphs below to compare possible different articulations of regulatory frameworks. In the case of the European Union, it must be borne in mind that this is a regional union and that regulation is thus the result of EU and member states' laws. In all cases, however, it must be noticed that the cybersecurity legislation supersedes neither existing legislation on communications or digital means nor legislation on data protection or privacy.

European Union: An Articulated System Involving Cooperation among Member States

Aside from provisions that can be traced in the regulation of financial markets to ensure integrity and risk management (see below), the European Union has already taken important specific steps to ensure cybersecurity and to increase trust in digital technologies.

In the first place, in 2016, as part of the EU Cybersecurity Strategy, the European Union's first legal act in the field of cybersecurity was adopted in the form of the NIS Directive. Directive 2016/1148[12] put in place requirements concerning national capabilities in the field of cybersecurity, established the first mechanisms to enhance strategic and operational cooperation between member states, and introduced obligations concerning security measures and incident notifications across sectors that are vital for the economy and society, such as energy, transport, the supply and distribution of drinking water, banking,[13] financial market infrastructures,[14] health care, digital infrastructure,

and key digital service providers (that is, search engines, cloud computing services, and online marketplaces).[15]

The NIS Directive has three main pillars, which underlie cooperation between member states. The NIS Directive lays down obligations for member states to designate national competent authorities, single points of contact, and computer security incident-response teams (CSIRTs) that perform tasks related to the security of network and information systems. The following are the three main pillars underlying such tasks:

1. National capabilities: EU member states must have certain national cybersecurity capabilities. For example, they must have a national CSIRT, perform cyber exercises and stress tests, and so on.
2. Cross-border collaboration: Cross-border collaboration between European countries—for example, the operational EU CSIRT network, the strategic NIS Cooperation Group, and so forth.
3. National supervision of critical sectors: EU member states must supervise the cybersecurity of critical market operators in their own countries: ex ante supervision in critical sectors (energy, transport, water, health, digital infrastructure, and finance sector) and ex post supervision for critical digital service providers (online marketplaces, cloud computing, and online search engines).

The European Union Agency for Cybersecurity (originally called the European Network and Information Security Agency, or ENISA) is tasked with supporting the cooperation of the CSIRTs. The CSIRTs are a network composed of EU member states. The European Commission participates in the network as an observer. In turn, ENISA is tasked with supporting the cooperation of the CSIRTs, and it provides the secretariat and active support for incident coordination upon request.[16] ENISA is a center of network and information-security expertise for the European Union, its member states, the private sector, and Europe's citizens, working with these groups since 2004 to develop advice and recommendations for good practice regarding information-security matters. It assists EU member states to implement relevant European legislation and works to improve the resilience of Europe's critical information infrastructure (CII) and networks. (The subsequent EU Cybersecurity Act, detailed below, strengthened the role of ENISA, including by making it a permanent agency for pan-European cybersecurity matters.)

The NIS Directive applies to operators of essential services and when a significant disruptive effect occurs. However, member states are responsible for determining which entities meet the criteria used to define operators of essential services. To ensure a consistent approach, all member states should apply the definition of "operator of essential services" consistently. To that end, the directive provides for the assessment of the entities active in specific sectors and subsectors, the establishment of a list of essential services, the consideration of a common list of cross-sectoral factors to determine whether a potential incident would have a significant disruptive effect, a consultation process involving relevant member states in the case of entities providing services in more than one member state, and the support of the NIS Cooperation Group in the identification process. Finally, member states are requested to submit to the European Commission the information necessary to assess the extent to which such common methodology allowed a consistent application of the definition by member states.

The NIS Directive recognizes the instruments already in place for cybersecurity in the financial markets and establishes a link between CSIRT cooperation and existing regulatory tools. The directive acknowledges that certain sectors of the economy are already regulated or may be regulated in the future by sector-specific EU legal acts that include rules related to the security of network and information systems. Whenever those EU legal acts contain provisions imposing requirements concerning the security of network and information systems or notifications of incidents, those provisions should apply if they contain requirements that are at least equivalent in effect to the obligations contained in the directive. Member states should then apply the provisions of such sector-specific EU legal acts and refrain from carrying out the identification process for operators of essential services as defined by the directive. Regulation and supervision in the sectors of banking and financial market infrastructures is highly harmonized at the EU level through the use of primary and secondary EU law and standards developed together with the European Supervisory Authorities (ESA). Within the banking union, the application and the supervision of those requirements are ensured by the single supervisory mechanism. (See the discussion below on the current draft directive and regulation on digital operational resilience for the financial sector.)

The NIS Directive does not affect the regime under EU law for the Eurosystem's oversight of payment and settlement systems. The directive acknowledges that operational risk is a crucial part of prudential regulation and supervision in the sectors of banking and financial market infrastructures, and that regulation and supervision covers all operations, including the security, integrity, and resilience of network and information systems. In respect to those systems, the requirements, which often exceed the requirements provided for under the directive itself, are set out in a number

of EU legal acts. These include the following: rules on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, and rules on prudential requirements for credit institutions and investment firms, which include requirements concerning operational risk; rules on markets in financial instruments, which include requirements concerning risk assessment for investment firms and for regulated markets; rules on over-the-counter derivatives, central counterparties, and trade repositories, which include requirements concerning operational risk for central counterparties and trade repositories; and rules on improving securities settlement in the European Union and on central securities depositories, which include requirements concerning operational risk. Furthermore, requirements for notification of incidents are part of normal supervisory practice in the financial sector and are often included in supervisory manuals. The directive thus concludes that member states should consider those rules and requirements as *lex specialis*, prevailing over the principles established by the directive. Moreover, the directive recommends that authorities responsible for oversight exchange experiences on matters concerning the security of network and information systems with the competent authorities under the directive. The same consideration applies to non-euro area members of the European System of Central Banks exercising such oversight of payment and settlement systems based on national laws and regulations.

In the second place, considering the increased cybersecurity challenges faced by the European Union, the Cybersecurity Act was adopted in 2018. Since a need was felt for a comprehensive set of measures that would build on previous EU action and foster mutually reinforcing objectives, and in the context of the positive development of the role of ENISA as a reference point within the framework of the European Union's new cybersecurity policy, the Cybersecurity Act transforms ENISA's mandate. Indeed, in light of the fast-evolving cyber threat landscape, it was felt that member states needed to be supported by a more comprehensive, cross-policy approach to building cyber resilience. To that end, it is the task of ENISA to promote the consistent implementation of the relevant legal framework—in particular, the effective implementation of Directive 2016/1148 and other relevant legal instruments containing cybersecurity aspects.

The Cybersecurity Act also establishes the European cybersecurity certification framework to ensure its implementation in a uniform manner in all member states to prevent "certification shopping" based on different levels of stringency across member states. The cybersecurity certification of ICT products, services, and processes was used in the European Union only to a limited extent. When it existed, it occurred mostly at the member state level or in the framework of industry-driven schemes. In that context, a certificate issued by a national cybersecu-

BOX 2

THE FRENCH NATIONAL CYBERSECURITY AGENCY

The French National Cybersecurity Agency (*Agence nationale de la sécurité des systèmes d'information*, ANSSI) is committed to making sure that public administrators, public service providers, and businesses can take full advantage of a secure and trustworthy digitalization. The role of ANSSI is to foster a coordinated, ambitious, proactive response to cybersecurity issues in France.[17]

The Military Programming Law[18] improved the ability of national public- and private-sector operators of vital importance to protect themselves and of ANSSI to support them in the event of a cyberattack. Article 22[19] of the law provided for the adoption of measures to step up the security of operators of vital importance and granted new prerogatives to the prime minister.

As the French coordinator for the transposition, ANSSI worked alongside all relevant stakeholders to prepare Decree 2018-384, which defines the cybersecurity framework for "operators of essential services" and "digital service providers."[20]

By choosing an ambitious transposition, France has established a list of sectors for essential services, following consultations by ANSSI with public and private stakeholders and its European partners. This list refers to many sectors, including banking and logistics.[21]

Finally, article 323 of the French *Code Pénal* identifies the different kinds of cybercrime and their penalties. As an example, according to article 323-1, the punishment for fraudulent access to an automated data-processing system is imprisonment and a fine up to €45,000.[22]

rity certification authority was not in principle recognized in other member states. Moreover, while new schemes are emerging, there seemed to be no coherent and holistic approach to horizontal cybersecurity issues. Some efforts had been made to ensure the mutual recognition of certificates within the European Union. However, they have been only partly successful. Therefore, it was felt that it was necessary to adopt a common approach and to establish a European cybersecurity certification framework that lays down the main horizontal requirements for European cybersecurity certification schemes to be developed and allows European cybersecurity certificates and EU statements of conformity for ICT products, services, or processes to be recognized and used in all member states.

Finally, a proposal for a directive on the resilience of critical entities is currently under discussion. On December 16, 2020, the European Commission issued a proposal on the resilience of critical entities[23] to enhance the resilience of critical entities providing essential services in the European Union. With this proposal, the commission intends to create an all-hazards framework to support member states in ensuring that critical entities can prevent, resist, absorb, and recover from disruptive incidents, no matter if they are caused by natural hazards, accidents, terrorism, insider threats, or public-health emergencies such as the one the world faces today. The proposal covers the following 10 sectors: energy, transport, banking, financial market infrastructures, health, drinking water, wastewater, digital infrastructure, public administration, and space. It includes provisions under which (a) member states would be obligated, among other things, to have a strategy for ensuring the resilience of critical entities, to carry out a national risk assessment, and, on this basis, to identify critical entities; (b) critical entities would be required to carry out risk assessments of their own, take appropriate technical and organizational measures to boost resilience, and report disruptive incidents to national authorities; and (c) critical entities providing services to or in at least one-third of member states would be subject to specific oversight, including advisory missions organized by the commission. The commission would offer different forms of support to member states and critical entities, an EU-level risk overview, best practices, methodologies, cross-border training activities, and exercises to test the resilience of critical entities.

The European Commission also simultaneously adopted a proposal for a revised NIS Directive. This proposal aims to ensure robust cyber resilience on the part of many entities by introducing more stringent supervision measures and enforcement. A list of administrative sanctions is established, including fines for breach of the cybersecurity risk-management and reporting obligations.[24] To ensure alignment between the two instruments, all critical entities identified under the critical entities' resilience directive would be subject to cyber resilience obligations under the revised NIS Directive.

Singapore: Requirements for Critical Information Infrastructure and Licensing of Providers of Cybersecurity Services

In 2018, a Cybersecurity Act entered into force in Singapore. The act establishes a legal framework for the oversight and maintenance of national cybersecurity in Singapore. The four key objectives of the act are (i) to strengthen the protection of CIIs[25] against cyberattack, (ii) to authorize the Cyber Security Agency (CSA) of Singapore to prevent and respond to cybersecurity threats and incidents, (iii) to establish a framework for sharing cybersecurity information, and (iv) to establish a light-touch licensing framework for cybersecurity service providers.[26] Although banking and finance is defined as a CII,[27] and in January 2021 the Monetary Authority of Singapore enhanced its technology risk-management guidelines to combat heightened cyber risks applying to all financial institutions, no specific regulation on CII related to the finance/banking sector seems to be foreseen in Singapore at this stage by the CSA or Monetary Authority of Singapore.[28]

The Singapore Cybersecurity Act focuses primarily on unauthorized (or, in any event, illicit) access and the integrity and confidentiality of information. According to the act, cybersecurity means the state in which a computer or computer system is protected from unauthorized access or attack and, because of that state, (a) the computer or computer system continues to be available and operational, (b) the integrity of the computer or computer system is maintained, and (c) the integrity and confidentiality of information stored in, processed by, or transmitted through the computer or computer system is maintained (section 2). The objective of the act is to ensure that all CIIs are maintained under such a status (which means that the risk of infrastructures not maintaining cybersecurity is mitigated to the maximum possible extent). In line with the definition of cybersecurity, the phrase "cybersecurity incident" means an act or activity that is carried out without lawful authority on or through a computer or computer system and that jeopardizes or adversely affects its cybersecurity or the cybersecurity of another computer or computer system.

A commissioner for cybersecurity (that is, the CSA) is appointed to oversee the cybersecurity of computers and computer systems. The commissioner has the duties and functions, among others, (i) to oversee and promote

the cybersecurity of computers and computer systems, (ii) to respond to cybersecurity incidents that threaten the national security, defense, economy, and foreign relations, (iii) to identify and designate CIIs and regulate owners of CIIs with regard to the cybersecurity of the CIIs, and (iv) to establish cybersecurity codes of practice and standards of performance for implementation by owners of CIIs.

The act strengthens the protection of CIIs against cyberattacks through a mechanism of designation. According to the act, a CII is a computer or a computer system for which a designation under the act is in effect. To that end, the act regulates the following actions: (i) designation of CIIs, (ii) the power to obtain information to ascertain if CIIs fulfill the criteria of a CII, (iii) withdrawal of the designation of a CII, (iv) furnishing of information relating to a CII, (v) establishment of codes of practice and standards of performance, (vi) the power to issue written directions, (vii) regulation of a change in ownership of a CII, (viii) the duty to report a cybersecurity incident in respect to a CII, and (ix) cybersecurity audits and risk assessments of CIIs. The CSA may designate the computer or computer system as a CII if the CSA is satisfied (a) that the computer or computer system is necessary for the continuous delivery of an essential service and that the loss or compromise of the computer or computer system would have a debilitating effect on the availability of the essential service in Singapore, and (b) that the computer or computer system is located wholly or partly in Singapore.

The commissioner has powers in line with oversight (and supervision) powers usually assigned to financial authorities. The act articulates the CSA's investigative powers and the corresponding duty of designated entities to inform the CSA. This includes the power of the CSA to send written directions when this is necessary or expedient for ensuring the cybersecurity of a CII or a class of CIIs, as well as the duty to report to the CSA cybersecurity incidents affecting a CII, cybersecurity audits, and risk assessments of CIIs. The owner of a CII who is aggrieved by a decision of the CSA has a right to appeal to the minister (who would rely on an advisory panel to that end).

Codes of practice or standards of performance have been issued by the commissioner for the regulation of owners of CIIs. The codes prescribe general requirements for CIIs, such as requirements on compliance, governance, identification, protection, monitoring and detection, cybersecurity incident response, cybersecurity awareness and information sharing, cybersecurity exercises, resiliency, and vendor management.[29] No specific requirements for the banking and finance sector have been issued so far by the CSA, whose major concern at this stage is cybersecurity risk in the global supply chain across all industries.[30]

Since 2016 and annually, the CSA has been publishing the *Singapore Cyber Landscape,* a publication that features facts and figures on key cyber threats and incidents in Singapore. As part of the CSA's cyber-awareness efforts,[31] the CSA has occasionally been issuing handbooks—such as *Cyber Safety Activity Books*,[32] an interactive cyber safety handbook,[33] and *Singapore's Safer Cyberspace Masterplan*[34]—as well as studies,[35] and it launched awareness campaigns.[36]

While the CSA guidance is general, the Monetary Authority of Singapore issued guidance to financial institutions in the form of notices and guidelines. These cover mostly cyber hygiene[37] and technology risk-management topics,[38] as well as risk-management practices, the provision of digital advisory services, insurers' own risk and solvency assessments, and online distribution of life policies.[39]

Cybersecurity service providers are licensed by the commissioner. No one may engage in the business of providing any licensable cybersecurity service to other persons unless it is duly licensed. Cybersecurity services are provided by a person for reward and are intended primarily for, or aimed at, ensuring or safeguarding the cybersecurity of a computer or computer system belonging to another person.[40] The CSA currently adopts a light-touch approach to license only two types of service providers: penetration testing, and the monitoring of managed security operations centers. These two services are prioritized because providers of such services have access to sensitive information from their clients. They are also relatively mainstream in the Singapore market and, hence, have a significant impact on the overall security landscape. The licensing framework seeks to strike a balance between security needs and the development of a vibrant cybersecurity ecosystem. The monitoring of managed security operations centers consists of monitoring the cybersecurity level of a computer or computer system of another person by acquiring, identifying, and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system. Penetration testing includes assessing, testing, or evaluating the cybersecurity level of a computer or computer system by searching for vulnerabilities in, and compromising, the cybersecurity defenses of the computer or computer system.

China: A Multilevel Cybersecurity-Protection System

China's first comprehensive privacy and security regulation for cyberspace, the Cybersecurity Law, came into force in June 2017. Prior to the enactment of the Cybersecurity Law, China already had some laws, rules,

and regulations relating to information security, such as Administrative Measures for Prevention and Treatment of Computer Viruses and Administrative Measures for Hierarchical Protection of Information Security. The Cybersecurity Law was adopted by the National People's Congress in November 2016, after a year of legislative proceedings, and came into force on June 1, 2017.[41] Following patterns similar to those of the Singapore Cybersecurity Act, the Cybersecurity Law includes general standards for information networks, a mechanism for designating CIIs, monitoring, early warning, and emergency response, as well as rules on data protection and (partially) on the identity of users. Covered CIIs are public communications and information services, energy, finance, transportation, water conservation, public services, and e-governance.[42]

A multilevel cybersecurity-protection system is established, under which all relevant network operators must respect general standards, while CIIs are covered by a designation mechanism. According to the requirements of the multilevel cybersecurity-protection system, all network operators must perform the following security-protection duties to ensure that the network is free from interference, damage, or unauthorized access and to prevent network data leaks, theft, or falsification: (a) formulate internal security-management systems and operating rules, determine which persons are responsible for cybersecurity, and implement responsibility schemes for cybersecurity protection; (b) adopt technical measures to prevent computer viruses, cyberattacks, network intrusions, and other actions endangering cybersecurity; (c) adopt technical measures for monitoring and recording operational statuses of the network and cybersecurity incidents and follow provisions to store network logs for at least six months; and (d) adopt such measures as data classification, backup of important data, and encryption. Network operators must also formulate emergency response plans for cybersecurity incidents and promptly address system vulnerabilities, computer viruses, cyberattacks, network intrusions, and other such cybersecurity risks. When cybersecurity incidents occur, network operators should immediately initiate an emergency response plan, adopt corresponding remedial measures, and report to the relevant competent departments in accordance with relevant provisions.

Self-regulation by relevant industry organizations is advocated by the law. Although the law states that the state establishes and improves a system of cybersecurity standards, it equally requests that relevant internet industry organizations, according to their articles of association, strengthen industry self-discipline, formulate cybersecurity norms of behavior, guide their members in strengthening cybersecurity protection according to the law, raise the level of cybersecurity protection, and stimulate the healthy development of the industry.

Additional standards are established for designated CIIs. In addition to the standards generally imposed on network operators, CII operators must also perform the following security-protection duties: (a) set up specialized security-management bodies and persons responsible for security management and conduct security background checks on those responsible persons and personnel in critical positions; (b) periodically conduct cybersecurity education, technical training, and skills evaluations for employees; (c) conduct disaster recovery backups of important systems and databases; and (d) formulate emergency response plans for cybersecurity incidents and periodically organize drills.

Rules on data protection are established for CIIs. Data is required to be stored within China. CII operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China are required to store it within mainland China. Where, due to business requirements, it is necessary to provide important data outside the mainland, CII operators must follow the measures jointly formulated by the state cybersecurity and IT departments and the relevant departments of the state council to conduct a security assessment. Moreover, network operators shall strictly maintain the confidentiality of the user information that they collect and establish and complete user information-protection systems. They must adopt technical and other necessary measures to ensure the security of the personal information that they gather and to prevent the leak, destruction, or loss of personal information. When personal information is or might have been leaked, destroyed, or lost, remedial measures shall be taken immediately and provisions followed to inform users promptly and to report to the competent departments in accordance with regulations.

No licensing is required for cybersecurity service providers, but they must respect relevant laws. Those providers carrying out cybersecurity certification, testing, risk assessment, or other such activities or publicly publishing cybersecurity information, such as system vulnerabilities, computer viruses, network attacks, or network incursions, must comply with relevant national provisions. No requirement for licenses yet appears to exist, as it is instead in Singapore.

Some rules on identity are established. Network operators handling network access and domain name registration

services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services must require users to provide real identity information when signing agreements with users or confirming the provision of services. In turn, the law commits the state to implement a network identity credibility strategy and to support research into and the development of secure and convenient electronic identity-authentication technologies, promoting reciprocal acceptance of different electronic identity-authentication methods.

Nigeria: A Cybersecurity Law with a Specific Chapter for the Financial Market

The Cybercrimes (Prohibition and Prevention) Act of 2015 established a comprehensive, legal, regulatory, and institutional framework in Nigeria to prohibit, prevent, detect, prosecute, and punish cybercrime. The objectives of the act are to provide an effective and unified legal, regulatory, and institutional framework for the prohibition, prevention, detection, prosecution, and punishment of cybercrimes, to ensure the protection of CIIs, and to promote cybersecurity and protect computer systems and networks, electronic communications, data and computer programs, intellectual property, and privacy rights.

To that end, the act establishes a designation mechanism for CIIs. As seen in Singapore and China, a mechanism for designating CIIs is established to permit the oversight of critical infrastructures. However, the relevant infrastructures are defined more widely than in other countries, and directions for standards are already contained in the act, rather than being left to a specific authority or state department. Indeed, the president designates certain computer systems and/or networks, whether physical or virtual, and/or the computer programs, computer data, and/or traffic data that are vital to the country and for which "*the incapacity or destruction of or interference with such system and assets would have a debilitating impact on security, national or economic security, national public health and safety, or any combination of those matters as constituting Critical National Information Infrastructure*" (article 3.1). The presidential order designating an entity may prescribe minimum standards, guidelines, rules, or procedures concerning (a) the protection or preservation of the CII; (b) the general management of the CII; (c) access to and transfer and control of data in any CII; (d) infrastructural or procedural rules and requirements for securing the integrity and authenticity of data or information contained in any designated CII; (e) the storage or archiving of data or information designated as a CII; (f) recovery plans in the event of disaster, breach, or loss of the CII or any part of it; and (g) any other matter required for the adequate protection, management, and control of data and other resources in any CII.

Criminal provisions are also contained in the act. These illustrate which behaviors are meant to be cyberattacks. The very long and detailed list of offenses include unlawful access to a computer; system interference; interception of electronic messages, email, or e-money transfers; tampering with critical infrastructure; willful misdirection of electronic messages; unlawful interceptions; computer-related forgery; computer-related fraud; theft of electronic devices; unauthorized modification of computer systems, network data, and system interference; cyber terrorism; identity theft and impersonation; child pornography and related offenses; cyberstalking; cybersquatting; racist and xenophobic offenses; breaches of confidence by service providers; phishing; spamming; spreading of computer viruses; and use of fraudulent devices or attached emails and websites.

Some offenses are specific to financial markets and payments. In fact, the long list of offenses also includes fraud related to electronic cards, using a card owned by another, the purchase or sale of a card owned by another, and fraudulently issuing e-instructions, as well as manipulating ATM/point-of-sale terminals. Furthermore, it is specifically stated that financial institutions,[43] as a duty to their customers, must put in place effective counterfraud measures to safeguard customers' sensitive information. However, where a security breach occurs, the burden of proving negligence lies on the customer—that is, to prove that the financial institution in question could have done more to safeguard the integrity of its information (article 19). (See below on the US Electronic Fund Transfer Act to see the application of a different policy choice that is established in a law on the instrument itself, rather than in the cybersecurity law.)

A specific part is devoted to financial institutions, imposing duties on them. Under the act, a financial institution must (a) verify the identity of customers carrying out electronic financial transactions by requiring the customers to present documents bearing their name, address, and other relevant information before issuing ATM cards, credit cards, debit cards, and other related electronic devices, and (b) apply know-your-customer principles when documenting customers before executing customers' electronic transfers, payments, or debit and issuance orders.

The National Security Adviser is the coordinating body for all security and enforcement agencies under the act,

which must also establish and maintain a National Computer Emergency Response Team Coordination Center responsible for managing cyber incidents in Nigeria. No independent authority exists in Nigeria, as in Singapore. The National Security Adviser has a coordination role to ensure consistency while managing a computer emergency response team as an autonomous center with specific functions for emergency response.

On the other hand, a Cybercrime Advisory Council is established, in charge of formulating and providing general policy guidelines for the implementation of the provisions of the act. The council comprises a representative from each of the following ministries, departments, and agencies: (a) Federal Ministry of Justice, (b) Federal Ministry of Finance, (c) Ministry of Foreign Affairs, (d) Federal Ministry of Trade and Investment, (e) Central Bank of Nigeria, (f) Office of the National Security Adviser, (g) Department of State Services, (h) Nigeria Police Force, (i) Economic and Financial Crimes Commission, (j) Independent Corrupt Practices Commission, (k) National Intelligence Agency, (l) Nigeria Security and Civil Defence Corps, (m) Defence Intelligence Agency, (n) Defence Headquarters, (o) National Agency for the Prohibition of Traffic in Persons, (p) Nigeria Customs Service, (q) Nigeria Immigration Service, (r) National Space Management Agency, (s) Nigerian Information Technology Development Agency, (t) Nigerian Communications Commission, (u) Galaxy backbone, (v) National Identity Management Commission, and (w) Nigeria Prisons Service, as well as (x) one representative each from the (i) Association of Telecommunications Companies of Nigeria, (ii) Internet Service Providers Association of Nigeria, (iii) Nigeria Bankers Committee, (iv) Nigeria Insurance Association, (v) Nigerian Stock Exchange, and (vi) a nongovernmental organization with a focus on cybersecurity.

2. OTHER LEGISLATIVE ACTS CONTAINING PROVISIONS RELEVANT TO THE CIA TRIAD

In several legal orders, laws (or regulations) addressing specific sectors of the economy also contain provisions directly addressing issues related to the security, integrity, or accessibility of systems and/or data. These are not cybersecurity law *per se* but contain provisions that complement those contained in cybersecurity laws, when they exist, or fill the gap, at least partially, when there is none. In the financial markets, in particular laws on electronic/digital instruments or products, some relevant aspects are regulated, such as authentication and/or authorization of transfers. In some cases, specific regulations exist for systems, which also include provisions on soundness. To the same extent, financial authorities, within their supervisory or oversight powers, may support resilience by imposing regulatory standards on regulated entities. Finally, customers' data is often protected under data-protection laws. Some of the many possible examples are illustrated below to permit the comparison of policy choices.

European Union: Data Protection and Lawfulness, Fairness, and Transparency

Many countries have a data-protection law. However, to gain a fully fledged understanding of legislation addressing issues relevant for cybersecurity, reference to a legal system that has already been described in many of its aspects seems preferable.

An important piece of the European legal framework concerns data security. The General Data Protection Regulation imposes obligations of lawfulness, fairness, and transparency onto organizations anywhere, so long as they target or collect data related to people in the European Union. This regulation lays down rules relating to the protection of natural persons regarding the processing of personal data.[44] Principles relating to the processing of personal data establish that the data must be (a) processed lawfully, fairly, and in a transparent manner in relation to the data subject ("lawfulness, fairness and transparency"); (b) collected for specified, explicit, and legitimate purposes ("purpose limitation"); (c) adequate, relevant, and limited to what is necessary in relation to the purposes for which the data is processed ("data minimization"); (d) accurate and, where necessary, kept up to date ("accuracy"); (e) kept in a form that permits the identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed ("storage limitation"); and (f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organizational measures ("integrity and confidentiality").

According to the regulation, it is necessary in particular to store and process data securely by implementing "appropriate technical and organizational measures." The organization must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including, among other things, as appropriate, (a) the pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services; (c) the ability

to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing.[45]

Moreover, the Data Protection Law Enforcement Directive ensures that the personal data of victims, witnesses, and suspects of crime is duly protected, and it facilitates cross-border cooperation in the fight against crime and terrorism. Directive (EU) 2016/680 on the protection of natural persons regarding the processing of personal data connected with criminal offenses or the execution of criminal penalties, and on the free movement of such data,[46] protects citizens' fundamental right to data protection whenever criminal law-enforcement authorities use personal data for law-enforcement purposes.

European Union: Legislation on Payment Services Also Covering Relationships between the Intermediary and Customer, as Well as New Services Embedding or Increasing Cyber Risk

The European Union has adopted several instruments that do not directly address cybersecurity *per se* but contain rules on the authentication and authorization of transfers and protection against attacks in the financial/payments sectors. As a first example, the 2007 Payment Service Directive (PSD) was upgraded into the directive commonly known as PSD2, which came into force in 2016 and was designed, among other things, to force providers of payment services to improve customer-authentication processes. To that end, PSD2[47] forces payment service providers to implement strong customer authentication, which involves the use of two authentication factors for bank operations where none was required previously, including payments and access to accounts online or via apps, as well as a stricter definition of what counts as an authentication factor.[48] This new piece of legislation has been read as a strong attempt to overcome the problem of the so-called man-in-the-middle attack, which requires the attacker to place itself between two communicating parties and relay messages for them while the parties believe they are communicating with each other directly and securely. The attacker can then monitor and possibly change the content of messages. The man-in-the-middle concept is not limited to computer security; similar attacks existed in the physical world long before computers.[49]

Moreover, PSD2 regulates and harmonizes two types of services not previously regulated in the European Union: payment initiation services and account information services, thus permitting the relevant authorities to monitor their operational risk, among other things. Account information services include the collection and storage of information from customers' different bank accounts in a single place, allowing customers to have a global view of their financial situation and making it easy to analyze their expenses and financial needs. Providers of payment initiation services facilitate the use of online banking to make payments online. These services help to initiate a payment from the consumer's account to the merchant's account by creating an interface to bridge both accounts, filling in the information needed for the bank transfer (that is, the amount of the transaction, account number, and message) and informing the store of the transaction. PSD2 also allows clients to make payments to a third party from a bank's app using any of the client's accounts (whether they belong to this entity or not). As an example, article 30 of PSD2 states: "*The personalized security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers. Payment initiation service providers do not necessarily enter into a contractual relationship with the account servicing payment service providers and, regardless of the business model used by the payment initiation service providers, the account servicing payment service providers should make it possible for payment initiation service providers to rely on the authentication procedures provided by the account servicing payments service providers to initiate a specific payment on behalf of the payer*." These entities must obtain a license to provide services and are thus subject to oversight, which includes monitoring of risk due to new actors, as well as their interaction with financial intermediaries. (See below for the role of authorities in this context and the issuance of secondary rules.)

United States: Legislation on Electronic Fund Transfers Covering Authentication and Authorization

In the United States, the Electronic Fund Transfer (EFT) Act of 1978, the primary legislation intended to protect individual consumers engaging in electronic fund transfers, regulates the authentication and authorization of transfers, among other things. EFT services include transfers through ATMs, point-of-sale terminals, automated clearinghouse systems, telephone bill-payment plans in which periodic or recurring transfers are contemplated, and remote banking programs.[50] The Federal Reserve Board implements the EFT Act[51] through Regulation E, which was issued by the Bureau of Consumer

Financial Protection and provides a basic framework that establishes the rights, liabilities, and responsibilities of participants in EFT systems.[52] These cover issues on the authentication and authorization of transfers that also allocate liabilities in case of fraud or mistake.

In the EFT Act's section on consumer liability and error resolution,[53] regulating the allocation of liability for unauthorized transfers, cybersecurity-related topics are considered as for allocation of liability. A consumer may be liable for an unauthorized EFT, depending on when the customer notifies the financial institution and whether an access device was used to conduct the transaction. No bright-line time limit is contained in the EFT Act within which consumers must report an unauthorized EFT.[54] More specifically, in case of the loss or theft of an access device, Regulation E defines three different timings of consumer notice to the financial institution[55] and three parallel maximum liability thresholds.[56,57] Furthermore, it prohibits greater liability in some circumstances, such as on account of the negligence of the consumer (for example, if he or she wrote a PIN on an ATM card). It is equally established that no agreement between the consumer and the financial institution may provide for greater liability, or that the consumer may be liable for a greater amount than under state law.[58]

Fund transfers are regulated by article 4A of the Uniform Commercial Code, which allocates liabilities in the case of mistake or fraud and approaches this issue based on the level of security chosen for the infrastructure processing the order. **The higher the level of security that the financial institution puts in place, the fewer responsibilities it is exposed to.** Article 4A describes a "security procedure" as one established by agreement of a customer and a receiving bank for the purpose of (i) verifying that a payment order or communication amending or cancelling a payment order is from the customer, or (ii) detecting an error in the transmission or the content of the payment order or communication. A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices (article 4A-201).[59] If a bank and its customer have agreed that the authenticity of payment orders issued to the bank in the name of the customer as sender will be verified pursuant to a security procedure, a payment order received by the receiving bank is effective as the order of the customer, whether authorized or not, if (i) the security procedure is a commercially reasonable method of providing security against unauthorized payment orders, and (ii) the bank proves that it accepted the payment order in good faith and in compliance with the security procedure and any written agreement or instruction of the customer restricting acceptance of payment orders issued in the name of the customer. The commercial reasonableness of a security procedure is a question of law to be determined by considering the wishes of the customer expressed to the bank, the circumstances of the customer known to the bank, including the size, type, and frequency of payment orders normally issued by the customer to the bank, alternative security procedures offered to the customer, and security procedures in general use by customers and receiving banks similarly situated. A security procedure is deemed to be commercially reasonable if (i) the security procedure was chosen by the customer after the bank offered, and the customer refused, a security procedure that was commercially reasonable for that customer, and (ii) the customer expressly agreed in writing to be bound by any payment order, whether authorized or not, issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer (article 4A-202).

II. Role of Authorities

From Financial Authorities Extending Their Functions to Strengthen Resilience to Fully Fledged Cybersecurity Authorities

Lacking fully fledged legislation on cybersecurity, existing authorities deal with (some) cybersecurity issues (at least provisionally) within their scope of competence and through secondary measures. Without a specific set of rules on cybersecurity, the powers of existing public entities might be stretched to permit the coverage of all aspects of cybersecurity (either expressly extending their powers or implicitly deriving them from existing supervision and/or oversight functions). Normally, such authorities will adopt standards to be applied directly to market operators and rely on existing monitoring functions to make them respected. Although their functions and activities might be either explicitly or implicitly expanded, their measures would still address exclusively entities under their powers. The institutional framework of the country would generally not permit the coverage of unregulated entities by the acts of such authorities.

However, when a cybersecurity law exists, a supervisory or oversight authority might still regulate the issue under its powers. In such a case, the authority will continue exercising its duties under existing legislation (unless the cybersecurity act specifically assigns it a specific role in the implementation of cybersecurity matters), but it will also be subject to the principles and standards established by the cybersecurity law. This occurs often in the financial sector, where the financial regulator extends its general policies on risk assessment to cyberattacks and acts consistently with its practice in monitoring any accident that occurs.

United States: Guidance of the New York Department of Financial Services

While a fully fledged federal law on cybersecurity does not exist in the United States, various federal and state laws do include provisions on cybersecurity. Competences by existing regulators to impose security requirements against cybercrimes derive from a variety of laws. Just to mention some, the Federal Trade Commission uses its enforcement authority in relation to unfair and deceptive practices to require companies to implement security measures. The Securities and Exchange Commission imposes disclosure requirements regarding cybersecurity risk and material cybersecurity incidents. The Gramm-Leach-Bliley Act requires financial institutions to implement written policies and procedures that are "reasonably designed" to ensure the security and confidentiality of customers' data. To the same end, many states have passed legislation imposing security requirements. The imposition of a standard of "reasonable security" seems to prevail.

The Cybersecurity and Infrastructure Security Agency Act of 2018 established a federal agency within the Department of Homeland Security with a coordination and information role for protecting critical infrastructures. The role of the agency is to coordinate between the government and the private sector by transmitting information and playing the role of a "risk advisor" (through capability delivery, operational collaboration, vulnerability management, capacity building, and cyber defense education and training). No role as a regulator is yet delegated to the Cybersecurity and Infrastructure Security Agency.

Within this context, the New York Department of Financial Services (DFS) issued a cybersecurity regulation effective from March 1, 2017. The regulation required all DFS-regulated entities, subject to certain exemptions, to adopt the core requirements of a cybersecurity program, including a cybersecurity policy, effective access privileges, cybersecurity risk assessments, and training and monitoring for all authorized users, among other requirements. The regulation also required the establishment of governance processes to ensure senior attention to these important protections. The purpose of the DFS cybersecurity regulation was to bolster the defenses of the financial-services industry against cybersecurity attacks, to protect markets and consumers' private information. The DFS declared that the governance framework set forth in the regulation was intended to assist in the bolstering of the industry's cybersecurity defenses for the protection of industry, overall markets, and consumers,

BOX 3

UNITED STATES: NEW YORK DEPARTMENT OF FINANCIAL SERVICES GUIDANCE AT THE TIME OF COVID-19

It is interesting to see how the financial regulator may address cybersecurity issues in a specific emergency situation, such as the pandemic. Indeed, the pandemic has disrupted normal operations in the financial-services industry and beyond, and cybercriminals are exploiting the crisis.

On April 13, 2020, New York DFS issued "Guidance to the Regulated Entities Regarding Cybersecurity Awareness during COVID-19 Pandemic." The DFS guidance touches on three main heightened risks of cyberattacks because of the crisis and recommends the following:

1. ***Remote working.*** Companies should make remote access as secure as possible under the circumstances. This includes the use of multifactor authentication and secure VPN connections that will encrypt all data in transit.

   As new devices, such as computers and phones, are acquired or repurposed for remote working, regulated entities should ensure that the devices are properly secured. Regulated entities that have expanded their bring-your-own-device policies to enable mass remote working should be aware of the security risks and consider mitigating steps. Some personal devices are not properly secured or are already compromised. Remote working has increased reliance on video- and audio-conferencing applications, but these tools are increasingly targeted by cybercriminals. Regulated entities should configure these tools to limit unauthorized access and make sure that employees are given guidance on how to use them securely. Employees may be using unauthorized personal accounts and applications, such as email accounts, to remain productive while working remotely.

2. ***Increased phishing and fraud.*** Regulated entities should remind their employees to be alert for phishing and fraud emails, and entities should revisit phishing training and testing at the earliest practical opportunity.

3. ***Third-party risk.*** The challenges created by the COVID-19 pandemic have also affected third-party vendors, and regulated entities should reevaluate the risks to critical vendors.

   The above recommendations are a specification of existing measures established by the DFS to ensure integrity and reinforce risk management by financial institutions. (See, for instance, 23 NYCRR §§ 500.12 and 500.15 and 23 NYCRR § 500.11, referred to in the guidance). In December 2020, as another attempt to alert financial institutions about potential risks related to COVID-19, the Financial Crimes Enforcement Network issued a notice about potential fraud, ransomware attacks, or similar types of criminal activity related to the COVID-19 vaccine and its distribution .

along with ongoing DFS oversight, including regular and target examinations. Consistent with these objectives, DFS examiners have been including cybersecurity in all regular examinations across the department. Furthermore, DFS established internal policies and procedures for the review of and response to confidential information provided to DFS by regulated entities as part of the regulation's notice and other procedures.

The final effective date for the regulation was March 1, 2019, by which time, under section 500.11, entities regulated by DFS were required to have written policies and procedures that are based on a risk assessment to ensure the security of nonpublic information and information systems that are accessed or held by third-party service providers. Accordingly, by March 1, 2019, all banks, insurance companies, and other financial-service institutions and licensees regulated by DFS were required to have a robust cybersecurity program in place designed to protect consumers' private data; a written policy or policies approved by the board of directors or a senior officer; a chief information-security officer to help protect data and systems; and controls and plans in place to help ensure the safety and soundness of New York's financial-services industry, including encryption and multifactor authentication.

The DFS regulation requires each entity to conduct an annual review and assessment. This concerns the achievements, deficiencies, and overall compliance with regulatory standards of each entity's cybersecurity program and requires certifying the institution's compliance with the regulation annually. The DFS compliance certification is a critical governance pillar for the cybersecurity program of all DFS-regulated entities.

Canada: An Authority to Service Government Bodies to Ensure Cybersecurity and Impose Individual Requirements on Individual Providers

Canada addresses cybercrimes, aside from the criminal code, by a series of sectoral laws, such as the Security Information Act and the Anti-Spam Act, as well as privacy statutes. The ensemble of rules in the various relevant laws grant protection to customers or systems according to the circumstances. No fully fledged legislation on cybersecurity yet exists at this stage.

The Cyber Centre is an operational authority for cybersecurity on certain projects, primarily within the Government of Canada. In these cases, clients must follow Cyber Centre directives. The center provides services and guidance to federal departments that require communication-security[60] solutions to protect their information. Federal departments requiring communication-security (COMSEC) material must establish a COMSEC account and appoint supporting COMSEC personnel. Their departmental security officer must submit a letter to COMSEC Client Services requesting the establishment of a COMSEC account.[61] Federal departments must also appoint appropriate COMSEC personnel to manage their departmental COMSEC program. A departmental COMSEC authority may be appointed by the departmental security officer to act in his/her stead to develop, implement, maintain, coordinate, and monitor the departmental COMSEC program, while a COMSEC custodian will be responsible for the generation, receipt, custody, distribution, disposition or destruction, and accounting of COMSEC material entrusted to their COMSEC account or subaccount.[62]

Australia: A Prudential Supervisory Authority Based on Existing Legislation Monitoring Cybercrime through Prudential Standards

The Australian Prudential Regulation Authority (APRA) is an independent authority that supervises institutions across banking, insurance, and superannuation and promotes financial-system stability in Australia. Within its powers, APRA published a 2020–24 Cyber Security Strategy that aims at helping improve the resilience of the country's financial system against cyber threat. Within such a context, APRA recently completed an independent assessment of the compliance by a pilot set of entities with CPS 234 of 2019, APRA's Information Security Prudential Standard.

APRA CPS 234 aims at ensuring that an APRA-regulated entity takes measures to be resilient against information-security incidents (including cyberattacks) by maintaining an information-security capability commensurate with information-security vulnerabilities and threats. The key requirements of this prudential standard are that an APRA-regulated entity must (i) clearly define the roles and responsibilities related to information security of its board, senior management, governing bodies, and individuals; (ii) maintain an information-security capability that is commensurate with the size and extent of threats to its information assets and that enables the continued sound operation of the entity; (iii) implement controls to protect its information assets commensurate with the criticality and sensitivity of those information assets and undertake systematic testing and assurance regarding the effectiveness of those controls; and (iv) notify APRA of material information-security incidents. APRA also issued a Prudential Practice Guide illustrating its expectation and best practice in implementation of the CPS 234.

BOX 4

THE HONG KONG ICAST: AN INTELLIGENCE-LED CYBERATTACK SIMULATION

Although Hong Kong has no fully fledged cybersecurity law, cybercrimes are addressed in laws whose provisions have been expanded to permit the prosecution of cybercrimes. Within such a context, sectoral regulators apply existing legislation to promote cyber resilience within the scope of their regulatory action. Financial authorities, such as the Securities and Futures Commission and the Hong Kong Monetary Authority, have issued specific guidelines that set out cybersecurity requirements to be adopted by licensees and financial institutions.

The Hong Kong Monetary Authority introduced the Cybersecurity Fortification Initiative in 2016, which aims to raise the cyber resilience of Hong Kong's banking system. The initiative is underpinned by three pillars: the Cyber Resilience Assessment Framework, the Professional Development Programme, and the Cyber Intelligence Sharing Platform. The initiative aims (i) to establish a common risk-assessment framework for banks, (ii) to offer training and certifications in cybersecurity, and (iii) to facilitate the sharing of cyber threat intelligence. At the end of 2020, the Hong Kong Monetary Authority launched an upgraded Cybersecurity Fortification Initiative 2.0, to streamline the process of assessing cyber resilience. Furthermore, it created an intelligence-led framework for simulating attacks, to support the core of its financial-services sector in becoming more cyber resilient.

iCAST is a regulatory requirement introduced by the Hong Kong Monetary Authority under the Cyber Resilience Assessment Framework. Banks aiming to attain "intermediate" or "advanced" maturity level under the cyber assessment must conduct iCAST. It is to be applied on top of the traditional penetration testing. Test scenarios are designed to replicate current real-life cyberattacks based on specific and up-to-date threat intelligence.

European Union: The European Supervisory Authorities, as Well as the European Central Bank Fight Cyber Risk within Their Competencies

The final guidelines on ICT and security risk management of the European Banking Authority (EBA) set out how financial institutions should manage the ICT and security risks to which they are exposed, and the guidelines provide financial institutions with a better understanding of supervisory expectations for the management of such risks. These most recent EBA guidelines[63] integrate and are built upon the requirements set out in previous guidelines—that is, the EBA guidelines on security measures.[64] Those guidelines were addressed to payment service providers and applied only to their payment services, but they were, in fact, relevant to a broader set of institutions. For that reason, the latest guidelines were formulated to be addressed to a broader range of financial institutions under the EBA's remit (namely, to credit institutions for all activities) and to investment firms.

The guidelines focus on the management and mitigation of ICT and security risks by establishing sound internal governance and an internal control framework that sets clear responsibilities for financial institutions' staff, including for the management bodies. The guidelines require the establishment of the financial institution's ICT strategy, the management and mitigation of ICT and security risks through an independent and objective control function, appropriately segregated from ICT operations processes and not responsible for any internal audit, and an independent internal audit function. They also remind financial institutions to ensure the effectiveness of the risk-mitigating measures, as defined by their risk-management framework, when outsourcing or using third-party providers. This should be set out in contracts and service-level agreements. Nevertheless, financial institutions should monitor and seek assurance of the level of compliance.

Specific requirements are imposed for payment service providers. This occurs by prescribing requirements for managing relationships with payment service users, including allowing users to disable specific payment functionalities (where product functionality permits) and to receive alerts about initiated and/or failed attempts to initiate payment transactions and providing users with assistance on questions and requests for support. The EBA stresses the importance of ensuring transparency, so payment service users always know which payment service provider is responsible for providing them with the payment service.

The EBA guidelines responded to the European Commission's FinTech Action Plan, which requested that the EBA develop guidelines on ICT risk-management and mitigation requirements in the EU financial sector. In March 2018, the European Commission adopted an action plan on fintech to foster a more competitive and innovative European financial sector.[65] The action plan sets out 19 steps that the commission intends to take to enable innovative business models to scale up at the EU level, to support the uptake of new technologies such as blockchain, artificial intelligence, and cloud services in the financial sector, and to increase cybersecurity and the integrity of the financial system. In this context, the commission invited the ESA[66] to map the existing supervisory practices around ICT security and governance requirements across financial sectors and, where appropriate, to consider issuing guidelines aimed at supervisory convergence and enforcement of ICT risk-management and mitigation requirements in the EU financial sector and, if necessary, to provide the commission with technical advice on the need for legislative improvements, as well as to evaluate the costs and benefits of developing a coherent cyber resilience testing framework for significant market participants and infrastructures within the whole EU financial sector.

To that end, the ESA issued two different pieces of joint advice. The ESA published two pieces of joint advice in response to requests made by the European Commission in its March 2018 FinTech Action Plan: a joint advice on the need for legislative improvements relating to ICT risk-management requirements in the EU financial sector,[67] and a joint advice on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector.[68]

In the joint advice on the need for legislative improvements relating to ICT risk-management requirements in the EU financial sector, the objective of the ESA was for every relevant entity to be subject to clear general requirements on the governance of ICT, including cybersecurity, to ensure the safe provision of regulated services. Guided by this objective, the proposals presented in the advice aimed at promoting stronger operational resilience and harmonization in the EU financial sector by applying changes to sectoral legislation. Incident reporting is highly relevant to ICT risk management and allows relevant entities and authorities to log, monitor, analyze, and respond to ICT operational, ICT security, and fraud incidents. Therefore, the ESA called for streamlining aspects of the incident-reporting frameworks across the financial sector. Furthermore, the ESA suggested consideration of a legislative solution for an appropriate oversight framework to monitor the activities of critical third-party service providers.

The second joint advice was on the costs and benefits of a coherent cyber resilience testing framework for significant market participants and infrastructures within the EU financial sector. Regarding the costs and benefits of a coherent cyber resilience testing framework, the ESA saw clear benefits of such a framework. However, they considered that at that time there were significant differences in the maturity level of cybersecurity across and within financial sectors. In the short term, the ESA advised focusing on achieving a minimum level of cyber resilience across the sectors that was proportionate to the needs and characteristics of the relevant entities. Furthermore, the ESA proposed establishing, on a voluntary basis, a coherent European Union–wide testing framework together with other relevant authorities considering existing initiatives, and with a focus on threat-led penetration testing. In the long term, the ESA aimed to ensure a sufficient cyber maturity level of identified cross-sector entities.

In their joint advice, the ESA acknowledged the need for widening their existing competences to perform expected activities on cybersecurity efficiently. To implement the proposed actions, the ESA highlighted the required legal basis and explicit mandate, which they meant to be necessary for the development and implementation of a coherent resilience testing framework across all financial sectors by the ESA in cooperation with other relevant authorities. Indeed, this led the European Commission to adopt a draft regulation on digital operational resilience for the financial sector. (See above.)

On its side, the ECB monitors cyber risk within its oversight functions over financial market infrastructures. As mentioned in the introduction, the ECB has implemented the CPMI-IOSCO guidance on cyber resilience. Moreover, as illustrated above, the NIS Directive does not affect the regime under EU law for the Eurosystem's oversight of payment and settlement systems. The ECB has thus developed an oversight approach to assess financial market infrastructures against the CPMI-IOSCO guidance, which it applies to all financial market infrastructures under its monitoring: the Cyber Resilience Oversight Expectations.

The ECB's Cyber Resilience Ovesight Expectations may also be used by domestic authorities, with the consequence of making it applicable also in the domestic legal order of member states. While the oversight of payment systems is a Eurosystem competence, in most countries of the euro area the oversight of clearing and settlement systems (that is, securities settlement systems or central securities depositories and central counterparties) is conducted by national central banks under national law competencies, often in cooperation with other national

authorities. In those cases, the ECB encourages national central banks and these other authorities to opt to use the Cyber Resilience Oversight Expectations for the financial market infrastructures under their oversight, in line with the applicable laws and regulations, to achieve the intended results. Such expectations are yet declared to be without prejudice to the application of all relevant domestic laws and regulations.

Singapore: A Fully Fledged Cybersecurity Agency

The role of the Singapore Cybersecurity Act has been described above. It is evident that the CSA plays a pivotal role in the implementation of the act and oversees activities in a way that closely resembles oversight in financial markets. The CSA's core mission is to keep Singapore's cyberspace safe and secure, to underpin the country's national security, power a digital economy, and protect users. In particular, to underpin national security, the CSA monitors cyberspace for cyber threats and oversees CIIs to ensure the continuous delivery of essential services. The agency assesses the risks that the threats pose and takes appropriate mitigation measures to prevent them. When cyberattacks succeed, the CSA puts in place incident-response teams that stand ready to investigate, contain, and remediate serious cyberattacks on CIIs. The CSA also regularly conducts cybersecurity exercises to ensure that the country's critical sectors are ready to respond promptly and effectively in the event of an attack.

The CSA is also responsible for creating a safer cyberspace for enterprises and individual end users. To that end, it advocates and practices security by design, provides security consultancy services to other government agencies, certifies products, and validates systems' security assurance. To power a digital economy, the CSA is building a vibrant cybersecurity ecosystem by working closely with the cybersecurity industry and universities to encourage cybersecurity innovation.

Besides the CSA, and despite the fact that no specific regulation on CII related to the finance/banking sector seems to be foreseen at this stage (see above), the Monetary Authority of Singapore plays an extremely relevant role in combating cybercrimes. As briefly mentioned above, the authority has recently enhanced its technology risk-management guidelines. The revised Technology Risk Management Guidelines set out technology risk-management principles and best practices for the financial sector, to help financial institutions establish sound and robust technology risk governance and oversight, maintain cyber resilience, and cope with new emerging technologies and shifts in the cyber threat landscape. In particular, the guidelines focus on cloud technologies, application programming interfaces, and rapid software developments. Furthermore, they request financial institutions to perform strict oversight of third-party service providers and impose upon them high duties of care and due diligence.

Nigeria: The Role of the Central Bank under a Fully Fledged Cybersecurity Act Not Contemplating a Newly Constituted Cybersecurity Authority

In Nigeria, the Cybersecurity Act of 2015 did not establish a fully fledged authority but a coordination system and an advisory body, permitting consistency and the joint development of cyber policy among relevant authorities. In that context, the central bank issued a few regulations on cybersecurity. In 2018, the Central Bank of Nigeria issued "Risk-Based Cybersecurity Framework and Guidelines for Deposit Framework and Payment Service Providers." On August 13, 2021, it further issued a draft of "Risk-based Cybersecurity Framework Guidelines for Other Financial Institutions."[69] Such draft guidelines regulate many aspects, including cybersecurity governance and oversight, cybersecurity risk-management systems, cyber resilience assessment, cybersecurity operational resilience, cyberthreat intelligence and metrics, and monitoring and reporting.

Despite the existence of the 2015 Cybersecurity Act, no mention of it is made in the Central Bank of Nigeria's guidelines. The measures adopted by the central bank resemble those of the EBA within the European Union (irrespective of the exact content of each of them). In both cases, the financial authority relies on its own powers and functions and builds its standards upon supervision and oversight practice in the financial sector. Of course, this does not mean that the Cybersecurity Act has no weight; its provisions need to be respected by financial institutions, and measures by the Central Bank of Nigeria cannot contradict them. However, the latter are filtered and expanded within the rationale of financial oversight.

III. Toward a Consolidated Approach Combining Financial Market Regulation and Cybersecurity Rules

THE EU DRAFT REGULATION ON DIGITAL OPERATIONAL RESILIENCE FOR THE FINANCIAL SECTOR

The European Commission's FinTech Action Plan took stock of the overlap between cybersecurity laws and policies and operational resilience. The plan acknowledged that fintech sits at the crossroads of financial services and the digital single market, and that there are important synergies between the commission's Digital Single Market Strategy, the European Union's cybersecurity strategy, the eIDAS Regulation, and financial-services initiatives such as the Consumer Financial Services Action Plan. It thus concluded that making the financial sector more cyber resilient is of paramount importance to ensure that it is well protected, that financial services are delivered effectively and smoothly across the European Union, and that consumer and market trust and confidence are preserved.

In light of the above, the European Commission issued a draft regulation on digital operational resilience in the financial markets that tackles cyberattacks through measures on resilience. Policy makers and supervisors have increasingly focused on risks stemming from reliance on ICT. They have notably tried to enhance firms' resilience by setting standards and through the coordination of regulatory or supervisory work. In line with this, the draft regulation is meant to enhance and streamline the financial entities' conduct of ICT management, establish a thorough testing of ICT systems, increase supervisors' awareness of cyber risks and ICT-related incidents faced by financial entities, and introduce powers for financial supervisors to oversee risks stemming from financial entities' dependence on third-party ICT service providers, as well as information and intelligence sharing. The proposal will also create a consistent incident-reporting mechanism that will help reduce administrative burdens for financial entities and strengthen supervisory effectiveness.

The legislative framework contemplated by the regulation and strengthening the digital operational resilience of EU financial entities is consistent with the policy objectives of the NIS Directive. The draft regulation would maintain the benefits associated with the horizontal framework on cybersecurity (for example, the NIS Directive) by keeping the financial sector within its scope. The financial sector would remain closely associated with the NIS cooperation body, and financial supervisors would be able to exchange relevant information within the existing NIS ecosystem. The initiative would be equally consistent with the European Critical Infrastructure Directive. Finally, this proposal is fully in line with the Security Union Strategy, which

called for an initiative on the digital operational resilience of the financial sector, given its high dependence on ICT services and its high vulnerability to cyberattacks.

In fact, the draft regulation addresses gaps of the NIS Directive. The NIS Directive applies to three types of financial entities: credit institutions, trading venues, and central counterparties. (See above.) However, since it sets out a mechanism for identifying operators of essential services at the national level, in practice only certain credit institutions, trading venues, and central counterparties identified by the member states are brought into its scope and thus required to comply with the ICT security and incident-notification requirements laid down in it. As the draft regulation raises the level of harmonization of digital resilience components by introducing requirements on ICT risk management and ICT-related incident reporting that are more stringent than those laid down in the current EU financial-services legislation, this constitutes an increase in harmonization over requirements laid down in the NIS Directive. Consequently, the draft regulation would constitute *lex specialis* to the NIS Directive.

To maintain a strong relationship between the financial sector and the European Union's horizontal cybersecurity framework, and to ensure consistency with the cybersecurity strategies already adopted by member states, financial supervisors would be made aware of cyber incidents affecting other sectors covered by the NIS Directive. The ESA and national competent authorities are expected to participate in the strategic policy discussions and the technical workings of the NIS Cooperation Group, respectively, to exchange information and cooperate further with the single points of contact designated under the NIS Directive. The competent authorities under the NIS Regulation should also consult and cooperate with the national CSIRTs designated in accordance with article 9 of Directive (EU) 2016/1148.

Provisions for the cyber resilience of systems and/or entities represent the way that financial authorities implement cybersecurity policies under the existing domestic legal frameworks, whether disposing of a fully fledged cybersecurity act or not. It is evident, on the one hand, that the ESA felt the need for a sound legal basis for their monitoring activities in relation to cybersecurity that would go beyond their general supervisory or oversight powers, but this was due to the need for coordination with other relevant authorities and the possibility of using the specific tools elaborated by the legislation on cybersecurity to defeat cyber risk (such as emergency responses). On the other hand, such activities are framed within the oversight of financial markets and focus on resilience, rather than on direct defense against individual cyberattacks. The same approach seems to have been adopted in Singapore (where the Monetary Authority of Singapore has the power to intervene in the financial sector, although it did not do so at this stage), as well as in Nigeria, just to mention two.

Conclusion

1. LESSONS LEARNED

From a comparative analysis of domestic (or regional) legal and/or regulatory frameworks addressing cybersecurity issues, it appears that only a few states have adopted a cybersecurity law. Cybersecurity is still a blurry concept to a great extent, so it is difficult to make a comprehensive list of even potential topics to be regulated. Moreover, while cybercrimes are defined in legislation at times, and several countries have indeed established sanctions for perpetrators, the means and instruments to reduce cyber risk are dealt with under different pieces of regulation.

In the first place, those countries that have a fully fledged cyberlaw also often establish a new agency in charge of monitoring the implementation of the law and issuing standards for service providers and those managing ICT infrastructures (frequently only those considered to be critical). In some cases, specific regulations, up to an autonomous licensing mechanism, might be established for those entities in the market that provide cybersecurity services. This latter element is due mainly to the fact that general standards for the mitigation of cyber risk are often high-level in nature and leave it to the market to reach the expected protection through the business models and practices that they prefer. To that end, service providers that offer IT solutions for protection need to be at least partially monitored.

However, even when a cybersecurity law is adopted, a few issues are left out and regulated by other means. Indeed, in the second place, existing authorities often deal with ICT/operational/cybersecurity risk management within their competences and establish standards to make operators and networks more resilient. This activity may complement those of the cybersecurity authority, when one is contemplated in the country. More often, especially when no cyber law exists, these authorities autonomously elaborate standards and monitoring mechanisms, following their usual approach and directions. This approach is surely found in financial markets: supervisory and oversight authorities monitor risks and establish standards to mitigate risk in a wide array of situations. This easily includes IT risk, which can then expand into cyber risk.

In the third place, cybersecurity also affects data. Consequently, many countries include provisions on the integrity and confidentiality of data in their data-protection acts. These provisions exclusively address treatment of data and consequently might end up being, on the one hand, insufficient for regulating cybersecurity attacks or, on the other hand, wider in scope than the legal issues covered, going further beyond cyber risk. This coexis-

tence is possibly also the reason why some definitions of cybersecurity also include aspects linked to transparency and transferability of data.

Finally, the authentication of digital identity and the authorization of transfers and transactions are equally linked to protection against cyberattacks. Provisions to that end are found in specific statutory acts on digital identity and digital signature, on the one side, and on laws regulating electronic or digital transfers and/or transactions, on the other. This latter approach is typical of financial markets and, in particular, of (electronic) payment instruments or payment services in general.

It appears clear that, irrespective of whether a country disposes of legislation on one area or the other, it is difficult to expect that a single piece of legislation could cover all relevant aspects of cybersecurity. On the other hand, the lack of a comprehensive and consistent set of rules across legal and regulatory acts might result in loopholes or the implementation of conflicting policies.

2. GUIDANCE ON THE REGULATION OF CYBERSECURITY IN THE FINANCIAL SECTOR

The above analysis and the lessons learned from the current regulation of cybersecurity in some countries lead to a recommendation for a consistent and fully fledged strategy on cybersecurity, which could lead, in turn, to a fully fledged statutory act. A statutory act on cybersecurity would delimit the scope of cybercrimes and of entities in need of general standards to mitigate and cope with risk. This may fall under the competence of ministries and authorities directly responsible for ICT and/or innovation.

When focusing specifically on the financial sector, different approaches may depend on whether a cybersecurity law, or at least a cybersecurity strategy, exists. In the affirmative case, financial authorities shall have to implement such principles within their general prudential and oversight framework. In the negative, they shall equally try to reach potentially the same goals, although while relying exclusively on their general competences. To that end, international standards may play a role by offering guidance to financial regulators and ensuring consistency, either by direct implementation by the authority itself or as benchmarks for domestic policy choices/moral suasion.

All of the above shall depend on the circumstances of the country and on existing provisions that affect the area (such as laws on data protection, electronic signatures, EFTs, and payment services). However, it seems that financial authorities should implement cybersecurity principles within the existing general framework on oversight of the sector, which would permit the adoption of measures to spur integrity, safety, and resilience in general. The cyber resilience of financial institutions and systems, especially if systemically relevant, supports broader financial-stability objectives. It is thus important that any policy on cybersecurity in financial markets links regulatory action to oversight and minds the relevance of cyber resilience for financial stability.

On the other hand, consistency should be stressed. Protection against cyberattacks needs to be combined with rules on allocation of risk, so that all relevant stakeholders bear the responsibility. Rules should ensure that the best possible precautionary measures are put in place. In this context, there is a need for adequate powers for the financial-sector regulator to oversee and regulate the financial sector's cybersecurity risk-management framework, taking into account rights and liabilities in the event of any cybersecurity event and in view of the implications that such a cybersecurity event could have for financial stability. The discussion on whether and how to allocate powers for the financial-sector regulator to oversee and regulate the financial sector's cybersecurity risk-management framework could be led in parallel with the discussion on the need for financial-sector-specific computer emergency response teams, as seen in some countries.

The adoption of a fully fledged cybersecurity law might be the last step of an itinerary. Also in that case, any measures adopted in preparation for the final issuance of a cybersecurity law should follow a preexisting and shared strategy for the country. Then, once a law is adopted, either a chapter on financial services could be included to highlight the specifics of such a sector (being financial infrastructures and entities critical to the market), or regulations could be adopted by financial authorities to reflect cybersecurity aims within those promoted by oversight.

Finally, cooperation, collaboration, and coordination between cybersecurity authorities and financial-market regulators should be ensured. This should occur at both the national and the international level. In fact, consistency can be assured only after the specifics of financial markets have been duly identified and cybersecurity standards have been applied to such financial-sector specifics in a way that ensures consistency with general cybersecurity principles, on the one hand, and oversight and regulatory stances in financial markets, on the other. Over the years, international standards have elaborated on forms and instruments of cooperation, and the CPMI-IOSCO guidance on cyber resilience stressed the need for cooperation to cope with cyber risk.

APPENDIX A

Glossary of Terms

Accountability: Property that ensures that the actions of an entity may be traced uniquely to that entity.

Asset: Something of either tangible or intangible value that is worth protecting, including people, information, infrastructure, finances and reputation.

Authenticity: Property that an entity is what it claims to be.

Availability: Property of being accessible and usable on demand by an authorized entity.

Compromise: Violation of the security of an information system.

Confidentiality: Property that information is neither made available nor disclosed to unauthorized individuals, entities, processes, or systems.

Cyber: Relating to, within, or through the medium of the interconnected information infrastructure of interactions among persons, processes, data, and information systems.

Cyber advisory: Notification of new trends or developments regarding a *cyber threat* to, or the *vulnerability* of, *information systems*. This notification may include analytical insights into trends, intentions, technologies, or tactics used to target *information systems*.

Cyber alert: Notification that a specific *cyber incident* has occurred or a *cyber threat* has been directed at an organization's *information systems*.

Cyber event: Any observable occurrence in an *information system*. *Cyber events* sometimes provide indication that a *cyber incident* is occurring.

Cyber incident: Whether resulting from malicious activity or not, a *cyber event* that either

i. Jeopardizes the *cyber security* of an *information system* or the information the system processes, stores, or transmits; or

ii. Violates the security policies, security procedures, or acceptable-use policies.

Cyber resilience: The ability of an organization to continue to carry out its mission by anticipating and adapting to *cyber threat*s and other relevant changes in the environment and by withstanding, containing, and rapidly recovering from *cyber incident*s.

Cyber risk: The combination of the probability of *cyber incidents* occurring and their impact.

Cybersecurity: Preservation of the confidentiality, integrity, and availability of information and/or information systems through the cyber medium. In addition, other properties, such as authenticity, accountability, nonrepudiation, and reliability can also be involved.

Cyber threat: A circumstance with the potential to exploit one or more *vulnerabilities* that adversely affects *cyber security*.

Data breach: *Compromise* of security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to data transmitted, stored, or otherwise processed.

Denial of service: Prevention of authorized access to information or *information systems*, or the delaying of *information-system* operations and functions, with a resultant loss of *availability* to authorized users.

Detect (function): Develop and implement the appropriate activities to identify the occurrence of a *cyber event*.

Distributed denial of service: A *denial of service* that is carried out using numerous sources simultaneously.

Exploit: Defined way to breach the security of *information systems* through *vulnerability*.

Identify (function): Develop the organizational understanding to manage *cyber risk* to *assets* and capabilities.

Incident-response team, also known as "computer emergency response team" or "computer security incident-response team": Team of appropriately skilled and trusted members of the organization who handle incidents during their life cycle.

Information sharing: An exchange of data, information, and/or knowledge that can be used to manage risks or respond to events.

Information system: Set of applications, services, information technology *assets,* or other information-handling components, which include the operating environment.

Integrity: Property of accuracy and completeness.

Multifactor authentication: The use of two or more of the following factors to verify a user's identity:

- Knowledge factor: something an individual knows
- Possession factor: something an individual has
- Biometric factor: something that is a biological and behavioral characteristic of an individual

Nonrepudiation: Ability to prove the occurrence of a claimed event or action and its originating entities.

Payment service provider: An entity that provides payment services, including remittances. Payment service providers include banks and other deposit-taking institutions, as well as specialized entities such as money transfer operators and e-money issuers

Penetration testing: A test methodology in which assessors, using all available documentation (for example, system design, source code, and manuals) and working under specific constraints, attempt to circumvent the security features of an *information system*.

Protect (function): Develop and implement the appropriate safeguards to ensure delivery of services and to limit or contain the impact of *cyber incidents*.

Recover (function): Develop and implement the appropriate activities to maintain plans for *cyber resilience* and to restore any capabilities or services that were impaired due to a *cyber incident*.

Reliability: Property of consistent intended behavior and results.

Respond (function): Develop and implement the appropriate activities to take action regarding a detected *cyber event*.

Social engineering: A general term for trying to deceive people into revealing information or performing certain actions.

Threat-led penetration testing, also known as "red team testing": A controlled attempt to compromise the *cyber resilience* of an entity by simulating the *tactics, techniques, and procedures* of real-life *threat actors*. It is based on targeted *threat intelligence* and focuses on an entity's people, processes, and technology, with minimal foreknowledge and impact on operations.

Vulnerability: A weakness, susceptibility, or flaw of an *asset* or control that can be exploited by one or more threats.

Endnotes

1. Cybersecurity and Infrastructure Security Agency, Security Tip (ST04-001), https://us-cert.cisa.gov/ncas/tips/ST04-001.
2. National Cyber Security Centre, "NCSC Glossary," https://www.ncsc.gov.uk/information/ncsc-glossary.
3. Regulation (EU) 2019/881 of the European Parliament and the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on Information and Communications Technology Cybersecurity Certification and Repealing Regulation (EU) No 526/2013 (Cybersecurity Act), https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN. Regulation 2019/881 repeals Regulation (EU) No. 526/2013.
4. 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
5. Although such definitions of cybercrimes are useful to understand the array of acts and behaviors against which the digital ecosystem should be protected, the extent to which criminal laws establish sanctions against cybercriminals is outside the scope of this study.
6. International Telecommunication Union, "Definition of Cybersecurity," https://www.itu.int/en/ITU-T/studygroups/com17/Pages/cybersecurity.aspx.
7. Financial Stability Board, Cyber Lexicon: "Preservation of *confidentiality, integrity* and *availability* of information and/or *information systems* through the *cyber* medium. In addition, other properties, such as *authenticity, accountability, non-repudiation* and *reliability* can also be involved. Source: Adapted from ISO/IEC 27032:2012," https://www.fsb.org/wp-content/uploads/P121118-1.pdf. However, it should be kept in mind that the lexicon is not intended for use in the legal interpretation of any international arrangement or agreement or any private contract.
8. The European Network and Information Security Agency (ENISA) tried to solve the puzzle of domestic definitions in 2015. The report *Definition of Cybersecurity: Gaps and Overlaps in Standardisation* summarizes and tries to provide order by considering the definitions of cybersecurity given by international organizations. See https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
9. NatLaw, "Working Paper on Best Practices for Electronic Collateral Registries," June 20, 2021, https://unidroitfoundation.org/wp-content/uploads/2021/07/bper-3.0-working-paper-on-collateral-registries-final.pdf.
10. Council of Europe, Convention on Cybercrime, Budapest, November 23, 2001, https://rm.coe.int/1680081561.
11. Cybercrime Prevention Act of 2012, Republic Act No. 10175, approved September 12, 2012.
12. 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, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC.
13. Credit institutions as defined in point (1) of article 4 of Regulation (EU) No. 575/2013 of the European Parliament and of the Council.
14. Operators of trading venues as defined in point (24) of article 4 of Directive 2014/65/EU of the European Parliament and of the Council, and central counterparties as defined in point (1) of article 2 of Regulation (EU) No. 648/2012 of the European Parliament and of the Council.
15. After the adoption of the NIS Directive in 2016, every European member state has started to adopt national legislation that implements the directive. EU directives give member states a level of flexibility to consider national circumstances—for example, to reuse existing organizational structures or to align with existing national legislation.
16. ENISA, https://www.enisa.europa.eu.
17. ANSSI, https://www.ssi.gouv.fr/en/mission/word-from-director-general/.

18. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
19. Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale.
20. Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
21. Décret n° 2018-384 du 23 mai 2018 relatif à la sécurité des réseaux et systèmes d'information des opérateurs de services essentiels et des fournisseurs de service numérique.
22. Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique. https://www.legifrance.gouv.fr/codes/id/LEGIARTI000006418316/2004-06-22.
23. European Commission, "Proposal for a Directive of the European Parliament and of the Council on the Resilience of Critical Entities," COM(2020) 829 final, https://ec.europa.eu/home-affairs/system/files/2020-12/15122020_proposal_directive_resilience_critical_entities_com-2020-829_en.pdf.
24. "Proposal for a Directive on Measures for High Common Level of Cybersecurity across the Union."
25. "'*[E]ssential service' means any of the following services: (a) services directly related to communications infrastructure, banking and finance, public utilities, public transportation, land transport infrastructure, aviation, shipping, or public key infrastructure*" (section 49).
26. Cybersecurity Act 2018, https://sso.agc.gov.sg/Acts-Supp/9-2018/.
27. First schedule: "*Services relating to banking and finance 12. Banking services, including cash withdrawal and deposits, corporate lending, treasury management, and payment services; 13. Payments clearing and settlement services; 14. Securities trading, clearing, settlement and depository services; 15. Derivatives trading, clearing and settlement services; 16. Services relating to maintenance of monetary and financial stability; 17. Currency issuance; 18. Services relating to cash management and payments for the Government*."
28. Cyber Security Agency of Singapore (CSA), Cybersecurity Act, https://www.csa.gov.sg/Legislation/Cybersecurity-Act.
29. Cybersecurity Act 2018 (Act 9 of 2018): Cybersecurity Code of Practice for Critical Information Infrastructure (First Edition—September 2018): Addendum No. 1—Dec. 2019, https://www.csa.gov.sg/-/media/Csa/Documents/Legislation_COP/cybersecurity-code-of-practice-cii-dec-2019.pdf.
30. CSA, "Speech by Mr. David Koh, Chief Executive, Cyber Security Agency of Singapore on 'Recent Cybersecurity Challenges, Dilemmas and Solutions from a National Perspective', at Israel Cyber Week 2021," July 21, 2021, https://www.csa.gov.sg/News/Speeches/israel-cyber-week-2021.
31. CSA, *Singapore Cyber Landscape*, https://www.csa.gov.sg/News/Publications.
32. CSA, Cyber Safety Activity Books, https://www.csa.gov.sg/News/Publications/Cyber-safety-activity-book.
33. CSA, *Cyber Safety: The Interactive Handbook,* https://www.csa.gov.sg/-/media/Csa/Documents/Publications/Cyber-Safety-Activity-Book-and-Handbook/Cyber-Safety-Handbook.pdf .
34. CSA, *Singapore's Safer Cyberspace Masterplan 2020*, https://www.csa.gov.sg/News/Publications/safer-cyberspace-masterplan.
35. CSA, *The IoT Security Landscape: Adoption and Harmonisation of Security Solutions for the Internet of Things*, https://www.csa.gov.sg/-/media/Csa/Documents/Publications/IoT_Security_Landscape/IoT-Security-Landscape-Report.pdf .
36. CSA, "CSA Launches Campaign to Continue to Drive Awareness and Adoption of Cybersecurity Practices," press release, June 28, 2021, https://www.csa.gov.sg/News/Press-Releases/csa-launches-campaign-to-continue-to-drive-awareness-and-adoption-of-cybersecurity-practices. CSA, SG Cyber Safe Seniors, https://www.csa.gov.sg/Programmes/sg-cyber-safe-seniors/about
37. Monetary Authority of Singapore (MAS), https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&page=1&q=cyber%20hygiene.
38. MAS, https://www.mas.gov.sg/regulation/regulations-and-guidance?content_type=Notices&topics=Risk%20Management%2FTechnology%20Risk&page=1&q=technology%20risk%20management.
39. MAS, https://www.mas.gov.sg/regulation/regulations-and-guidance?topics=Risk%20Management%2FTechnology%20Risk&content_type=Guidelines&page=1&q=technology%20risk%20management%20guidelines.
40. These include the following: (a) assessing, testing, or evaluating the cybersecurity of A's computer or computer system by searching for vulnerabilities in and compromising the cybersecurity defenses of the computer or computer system; (b) conducting a forensic examination of A's computer or computer system; (c) investigating and responding to a cybersecurity incident that has affected A's computer or computer system by conducting a thorough scan and examination of the computer or computer system to identify and remove elements relating to, and identify the root cause of, the cybersecurity incident, and that involves circumventing the controls implemented in the computer or computer system; (d) conducting a thorough examination of A's computer or computer system to detect any cybersecurity threat or incident that may have already penetrated the cybersecurity defenses of the computer or computer system, and that may have evaded detection by conventional cybersecurity solutions; (e) designing, selling, importing, exporting, installing, maintaining, repairing, or servicing one or more cybersecurity solutions; (f) monitoring the cybersecurity of A's computer or computer system by acquiring, identifying, and scanning information that is stored in, processed by, or transmitted through the computer or computer system for the purpose of identifying cybersecurity threats to the computer or computer system; (g) maintaining control of the cybersecurity of A's computer or computer system by effecting management, operational, and technical controls for the purpose of protecting the computer or computer system against any unauthorized effort to adversely affect its cybersecurity; (h) assessing or monitoring the compliance of an organization with the organization's cybersecurity policy; (i) providing advice in relation to cybersecurity solutions, including providing advice on a cybersecurity program or identifying and analyzing cybersecurity threats and providing advice on solutions or management strategies to minimize the risk posed by cybersecurity threats; (j) providing advice in relation to any practices that can enhance cybersecurity; and (k) providing training or instruction in relation to any cybersecurity service, including the assessment of the training, instruction, or competencies of another person in relation to any such activity (section 2).
41. Cybersecurity Law of the People's Republic of China, 2017 (translation into English by R. Creemers, P. Triolo and G. Webster), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/.
42. Article 31: "*The State implements key protection on the basis of the cybersecurity multi-level protection system for public communication and information services, power, traffic, water resources, finance, public service, e-government, and other critical information infrastructure which—if destroyed, suffering a loss of function, or experiencing leakage of data—might seriously endanger national security, national welfare, the people's livelihood, or the public interest. The State Council will formulate the specific scope and security protection measures for critical information infrastructure*."
43. The definition of a financial institution is extremely wide. It includes "any individual, body, association or group of persons, whether corporate or unincorporated which carries on the business of investment and securities, a discount house, finance company and money brokerage whose principal object includes factoring project financing, equipment leasing, debt administration, fund management, private ledger services, investment management, local purchase order financing, export finance, project consultancy, financial

consultancy, pension fund management, insurance institutions, debt factorization and conversion firms, dealer, clearing and settlement companies, legal practitioners, hotels, casinos, bureau de change, supermarkets and such other businesses as the Central Bank or appropriate regulatory authorities may, from time to time, designate." The act also contains definitions of "card," "electronic transfer of funds," and "financial transaction" (as well as related definitions).

44. Regulation (EU) 2015/2366 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), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=IT.
45. For the purposes of the General Data Protection Regulation, "personal data" means any information relating to an identified or identifiable natural person ("data subject"), while "processing" means any operation or set of operations that are performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. In turn, "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.
46. Directive (EU) 2016/680 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 by Competent Authorities for the Purposes of the Prevention, Investigation, Detection or Prosecution of Criminal Offences or the Execution of Criminal Penalties, and on the Free Movement of Such Data, and Repealing Council Framework Decision 2008/977/JHA.
47. Directive (EU) 2015/2366 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 (EU) No 1093/2010, and Repealing Directive 2007/64/EC (Text with EEA Relevance), OJ L 337, 23.12.2015, 35–127. The repealed directive is Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on Payment Services in the Internal Market Amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and Repealing Directive 97/5/EC.
48. Directive (EU) 2015/2366 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 (EU) No 1093/2010, and Repealing Directive 2007/64/EC, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L2366&from=IT.
49. ENISA, "Man-in-the-Middle," https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/man-in-the-middle.
50. Federal Reserve Board, Electronic Fund Transfer Act, 3, https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf.
51. Federal Reserve System, 12 CFR Part 205, Electronic Fund Transfers; Final Rule, *Federal Register* 71, no. 6 (January 10, 2006): 1638, https://www.govinfo.gov/content/pkg/FR-2006-01-10/pdf/06-145.pdf.
52. Consumer Financial Protection Bureau, 12 CFR Part 1005.1 Authority and Purpose (Regulation E), 2000, https://www.consumerfinance.gov/rules-policy/regulations/1005/1/.
53. Page 10.
54. Federal Reserve Board, Electronic Fund Transfer Act, 11, https://www.federalreserve.gov/boarddocs/caletters/2008/0807/08-07_attachment.pdf.
55. Within two business days of learning of a loss or theft; more than two business days after learning of a loss or theft up to 60 calendar days after the transmittal of a statement showing the first unauthorized transfer made with an access device; and more than 60 days after the transmittal of a statement showing the first unauthorized transfer made with an access device.
56. Lesser of $50, lesser of $500, and unlimited.
57. Page 12.
58. Page 11.
59. Comparing a signature on either a payment order or a communication with a customer's authorized specimen signature is not by itself a security procedure.
60. Communication security (COMSEC) is the discipline of preventing unauthorized access to telecommunications information in readable form while still delivering the information to the intended recipients. COMSEC comprises multiple disciplines, including cryptographic security, emission security, transmission security, and physical security, https://cyber.gc.ca/en/glossary/COMSEC.
61. Communication Security Establishment, Government of Canada, "IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network," ITSD04A, January 30, 2017, https://cyber.gc.ca/sites/default/files/publications/itsd-04a-eng.pdf.
62. Communication Security Establishment, Government of Canada, "IT Security Directive for the Management of CSE-Approved Cryptographic Equipment and Key to Secure a Telecommunications Network," ITSD04A, January 30, 2017, https://cyber.gc.ca/sites/default/files/publications/itsd-04a-eng.pdf.
63. EBA/GL/2019/04, November 28, 2019.
64. Guidelines on the Security Measures for Operational and Security Risks of Payment Services under Directive (EU) 2015/2366 (PSD2), EBA/GL/2017/17.
65. European Commission, *FinTech Action Plan: For a More Competitive and Innovative European Financial Sector*, COM/2018/0109 final, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0109.
66. All European Supervisory Authorities (that is, the European Banking Authority, European Securities and Markets Authority, and European Insurance and Occupational Pensions Authority) fight cyber risk within their competences and attempt to be consistent by issuing either parallel or joint documents.
67. JC 2019 26, April 10, 2019.
68. JC 2019 25, April 10, 2019.
69. Pursuant to the Banks and Other Financial Institution Act of 2020, other financial institutions now include international money-transfer services, financial holding companies, and payment service providers, among others.

THE WORLD BANK
IBRD • IDA | WORLD BANK GROUP