G20/OECD Task Force on Financial Consumer Protection

Compendium of Effective Approaches for Financial Consumer Protection in the Digital Age:

FCP Principles 1, 2, 3, 4, 6, 7, 8 and 9

Compendium of Effective Approaches for Financial Consumer Protection in the Digital Age: FCP Principles 1, 2, 3, 4, 6, 7, 8 and 9 3

Introduction and Policy Context 3
Overarching policy considerations 5
Principle 1: Legal, Regulatory and Supervisory Framework 7
Principle 2: Role of Oversight Bodies 21
Principle 3: Equitable and Fair Treatment of Customers 31
Principle 4: Disclosure & Transparency 35
Principle 6: Responsible Business Conduct of Financial Services Providers and Authorised Agents 39
Principle 7: Protection of Consumer Assets against Fraud and Misuse 46
Principle 8: Protection of Consumer Data and Privacy 57
Principle 9: Complaints Handling and Redress 63

Compendium of Effective Approaches for Financial Consumer Protection in the Digital Age: FCP Principles 1, 2, 3, 4, 6, 7, 8 and 9

Introduction and Policy Context

In an increasingly digital environment for financial products and services with the potential to support greater financial inclusion and inclusive growth, the need for effective financial consumer protection is more important than ever. At the same time, the policies and approaches developed and adopted by financial consumer protection authorities need to evolve and adapt in line with the environment.

In light of this, a key workstream of the G20/OECD Task Force on Financial Consumer Protection ("the Task Force") is to consider the implications for policy makers, oversight bodies and financial consumers of ever greater digitalisation of financial services in terms of financial consumer protection policy and the regulatory challenges and opportunities arising from financial innovation.

Among other things, the Task Force is responsible for the High-Level Principles on Financial Consumer Protection ("the Principles"), which set out the foundations for a comprehensive financial consumer protection framework. The Principles have been adopted by the OECD and endorsed by the G20.

While the Principles set out the foundations, they are supported by relevant, practical and evidence-based guidance and examples about how they can be implemented in the form of Effective Approaches. The Effective Approaches, which are based on approaches in use or being trialled in different jurisdictions, support jurisdictions to learn from each other and share insights, and provide a "tool box" of policy options on how to enhance financial consumer protection.

It is essential that the Effective Approaches are kept up to date in line with market, technological and legal developments. Among other things, therefore, the Task Force is progressively updating the effective approaches to take account of the increasingly digital environment.

As a first step, in 2017/18 the Task Force focussed on developing updated effective approaches for the implementation of Principles 2 (Role of Oversight Bodies) and Principle 4 (Disclosure and Transparency). Given the focus of the Argentinian G20 Presidency on digitisation in 2018, this work formed the basis of a *G20/OECD Policy Guidance Note on Financial Consumer Protection in the Digital Age*, published in July 2018 following the G20 Central Bank Governors and Finance Ministers meeting in Buenos Aires.1

In 2019, the focus turned to developing updated effective approaches to support the following Principles:

- Principle 1: Legal, Regulatory and Supervisory Framework

[1] The Policy Guidance Note was also an Input Paper for the G20 Policy Guide, *Digitisation and Informality*, endorsed by G20 Central Bank Governors and Finance Ministers in July 2018.

- Principle 3: Equitable and Fair Treatment of Customers
- Principle 6: Responsible Business Conduct
- Principle 9: Complaints Handling and Redress

The updated effective approaches were approved by the Task Force at its meeting in March 2019.

In 2020, the Task Force developed updated effective approaches to support the following Principles:

- Principle 7: Protection of Consumer Assets against Fraud and Misuse
- Principle 8: Protection of Consumer Data & Privacy.

The updated effective approaches for Principles 7 and 8 are also set out in a standalone OECD Policy Guidance Note on *Financial Consumer Protection Policy Approaches: protecting consumers' assets, data and privacy*, published in December 2020.

This document is a consolidated Compendium of all the updated effective approaches and jurisdiction examples relating to Principles 1, 2, 3, 4, 6, 7, 8 and 9.

Box 1. Digital financial services

This note adopts the working definition of digital financial services contained in the G20/OECD Report on ensuring financial education and consumer protection for all in the digital age:

Digital financial services (DFS) can be defined as financial operations using digital technology including electronic money, mobile financial services, online financial services, i-teller and branchless banking, whether through bank or non-bank institutions. DFS can encompass various monetary transactions such as depositing, withdrawing, sending and receiving money, as l aswell las other financial products and services including payment, credit, saving, pensions and insurance. DFS can also include non-transactional services, such as viewing personal financial information through digital devices. (OECD 2017)

Box 2. Artificial Intelligence

Artificial Intelligence (AI) is increasingly used and embedded in the development of digital financial products and services. An AI system may be defined as a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems are designed to operate with varying levels of autonomy. (OECD/LEGAL/0449)

In May 2019, the OECD published the OECD Principles on Artificial Intelligence, which are designed to promote AI that is innovative and trustworthy and that respects human rights and democratic values. The Principles were adopted in May 2019 by OECD member countries when they approved the OECD Council Recommendation on Artificial Intelligence. The OECD AI Principles also open to adherence by non-OECD member jurisdictions.

The OECD AI Principles

The Recommendation identifies five complementary values-based principles for the responsible stewardship of trustworthy AI:

- AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
- AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
- There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
- AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
- Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

Overarching policy considerations

There are a number of overarching considerations that policy makers should take into account when implementing or applying financial consumer protection approaches in the digital environment. These overarching considerations are relevant to the implementation of all Principles.

- Ensuring that regulatory responses are neutral in terms of the way that a product or service is distributed (i.e. the principle of "technological neutrality").
- Ensuring that regulatory responses reflect the business model, size, systemic significance, as well as the complexity and cross-border activity of the regulated entities (i.e. proportionality).
- Wherever practicable, using insights gained from data analysis to ensure an evidence-based approach to understanding market issues, policy and decision-making and understanding of the behaviour of consumers, including consumers who may be vulnerable, and market participants.
- Aiming to strike the right balance between the potential benefits to financial consumers when considering new business or distribution models and maintaining an appropriate degree of financial consumer protection.
- Maintaining flexibility, adaptability and continuous learning in a rapidly evolving and dynamic environment.
- Co-operation with other policy makers and oversight bodies, including those responsible for data protection and non-financial sectors such as telecommunications, to promote consistency where appropriate.

Box 3. RegTech and SupTech

In adapting to an increasingly digitalised environment for financial products and services, oversight bodies and financial institutions around the world are considering the use and application of regulatory technology ("RegTech") and supervisory technology ("SupTech").

While there are no single definitions of these terms, RegTech generally relates to the use of technology by regulated entities to comply with their regulatory and compliance requirements more effectively and efficiently. SupTech refers to the use of technology by oversight bodies for operations such as market surveillance and risk identification and monitoring.

While use of technology in relation to compliance and regulation is not new, more recent developments such as the increasing digitalisation of the financial services sector due to the drop in cost of computing power and storage and increasing capacity, means RegTech and SupTech are developing rapidly. They can include the use of artificial intelligence, machine learning and natural language processing, data reporting, regulatory codification and big data analysis technologies.

The Adoption of RegTech within the Financial Services Industry: Ten years from the Start of the 'Great Financial Crisis'; ESMA, May 2017

Principle 1: Legal, Regulatory and Supervisory Framework

Financial consumer protection should be an integral part of the legal, regulatory and supervisory framework and should reflect the diversity of national circumstances and global market and regulatory developments within the financial sector.

Regulation should reflect and be proportionate to the characteristics, type and variety of the financial products and consumers, their rights and responsibilities and be responsive to new products, designs, technologies and delivery mechanisms. Strong and effective legal and judicial or supervisory mechanisms should exist to protect consumers from and sanction against financial frauds, abuses and errors.

Financial services providers and authorised agents should be appropriately regulated and/or supervised, with account taken of relevant service and sector specific approaches.

Relevant non-governmental stakeholders – including industry and consumer organisations, professional bodies and research communities – should be consulted when policies related to financial consumer protection and education are developed. Access of relevant stakeholders and in particular, consumer organisation to such processes should be facilitated and enhanced.

1. The legal and regulatory framework should be based, among other things, on the principle of technological neutrality making sure it is capable of adapting to change and innovation while maintaining an appropriate level of financial consumer protection. At the same time, the legal and regulatory framework should be capable of addressing risks specific to the digital ecosystem.

> Example: in March 2018, South Africa implemented the Financial Sector Regulation Act (FSR Act) creating a Twin Peaks model of regulation. A new conduct regulator (Financial Sector Conduct Authority) has been established as of 1 April 2018, and has full scope of jurisdiction over the financial sector. The FSR Act allows for new financial products and services to be designated through regulation, which will bring the new products and services under regulation from both a customer protection and prudential perspective. The FSCA has jurisdiction over retail banks,,, a sector that had been under-regulated from a market conduct perspective. To inform the FSCA's supervision of bank conduct, and setting of conduct standards, a multifaceted approach will be taken. This includes engaging with government, the central bank and the Prudential Authority to coordinate work where there is shared interest. Focus areas include governance frameworks, fintech innovations affecting banks and conduct-related aspects of payment services.
>
> Example: to foster market integrity, financial stability and collective consumer protection the Federal Financial Supervisory Authority of Germany (BaFin) is open to new technologies and innovative business concepts, without giving them preferential treatment and thus avoiding a pro-innovation bias. Financial regulation and supervision in Germany is technology open/neutral. It embraces the principle of "same business, same risks, same rules" and combines it with a proportionate supervisory approach.
>
> Example: from April 2017, the Japan Financial Services Agency introduced a registration framework for broker-dealers of crypto-assets for legal tender and required such dealers to conduct identity verification of users and introduced

certain provisions to ensure user protection such as the provision of information to users.

Example: The Central Bank of Portugal has been particularly active in monitoring and supervising the sale of retail banking products and services through digital channels. One of the main goals of this activity is the promotion of technological neutrality, i.e., that consumer protection online is not less than offline. The Central Bank of Portugal's attention has been focused on consumer credit and current accounts sold through digital channels (homebanking, online platforms and apps). Regarding consumer credit, the central bank established reporting duties, requiring institutions to provide information on the credit they are selling through those channels (Circular Letter no. 4/2018). Thus, the central bank is able to monitor and supervise the marketing of consumer credit via digital channels so as to ensure respect for the rights of bank customers, in particular in the access to pre-contractual and contractual information. It was also adjusted the creditworthiness assessment's framework concerning this type of credit, allowing using indirect methods for credits up to an established amount, granting more convenience to the process. As for current accounts, the Central Bank of Portugal also amended the regulatory framework applicable to the opening of those accounts, allowing institutions to use assisted videoconferencing as an alternative form of proof of bank customers' identification. It allows the opening of accounts exclusively through digital channels. This amendment created conditions for greater competition in the market, while guaranteeing convenience and security.

2. Policy makers should monitor market trends and changes brought in retail financial services by digitalisation with a view to ensure the legal and regulatory framework is up-to-date and appropriately protects consumers. Particular attention should be paid at looking at how changes in the market are impacting consumers' behaviour.

Example: the European Commission has launched a behavioural study aimed at looking at the impact of the digitalisation of marketing and distance selling of retail financial services on consumers. The study will notably focus on how information is disclosed in the online environment and whether remedies exist to ensure that consumers are adequately protected, informed and can make the best choice of offers.

Example: German BaFin issued the study "Big Data meets artificial intelligence" to prepare discussions about the different issues surrounding big data and artificial intelligence from a supervisory and regulatory perspective. The study focusses on BDAI in the banking, insurance and capital market sectors, while also providing relevant information on how the consumers, who provide the data, are affected by the new technology driven approaches.

Example: The Central Bank of Portugal has been monitoring developments on the commercialisation of banking products and services on digital channels in Portugal. After a first questionnaire to institutions on products and services on digital channels and the publication of the results in 2016, in December 2018, a second questionnaire was launched. With this survey Banco de Portugal intends to assess the evolution of digital financial services in Portugal, the levels of adoption and use by customers, the constraints and obstacles to the

demand for digital channels and the main risks associated with the provision of financial services through digital channels.

Also, in order to monitor and oversee the commercialization of consumer credit products the Central Bank of Portugal required institutions (Circular Letter no. 4/2018) to provide information on the credit they are selling through homebanking, online platforms and apps. Based on the information reported, the central bank has been reflecting with institutions on the requirements applicable to consumer credit products and also considering behavioral economics' insights. As an example, concerning the disclosure of pre-contractual and contractual information to clients, the Central Bank of Portugal assesses the moment when the client acknowledges the main characteristics of the credit product and how it can select the most appropriate conditions for his preferences. It is also assessed whether mechanisms for adequate viewing and reading by the customer are implemented, in particular if they ensure the mandatory scroll down.

3. Policy makers should have in place a process for reviewing whether there may be existing regulatory policies, rules or practices may be interpreted as hindrances or barriers to competition and financial innovation. For example, regulation can be complex, hard to understand and slow to adapt to new business models or innovation. Regulatory uncertainty or complexity in licensing processes can deter businesses from entering the financial services market, therefore regulations in this regard should be proportionate and flexible, while at the same time, appropriate consumer and investor protection requirements should be maintained.

Example: in Hong Kong, the Hong Kong Monetary Authority (HKMA) has set up an internal taskforce to identify and streamline regulatory and other frictions to digital banking services. The taskforce has reached out to the banking industry as well as technology community engaged in the provision of financial services to hear their views on what changes need to be made to the regulatory requirements and practices. In 2018, the taskforce streamlined regulatory requirements in relation to remote onboarding, online finance, and online wealth management.

Example: the HKMA launched Balanced and Responsive Supervision Programme in 2017 in order to further enhance the supervisory interface with the banking sector. The aim is to drive a more effective supervisory outcome as well as establish a more conducive environment for banking development as underpinned by a proportionate and risk-based supervisory approach. Under this programme, the HKMA conducted a holistic review of the investor protection measures, with aims to enhance customer experience, facilitate market development while accord an appropriate degree of investor protection.

Example: in Italy, in accordance with EU standards, every new Bank of Italy regulatory measure must first be subject to stakeholder consultation, including consultation with industry and consumers' associations. To this end, draft regulations are published on websites, together with a cost-benefit analysis describing the impact on existing regulation, on the activities of market participants and the interest of financial consumers. Feedback statements are provided at the end of the consultation period.

Example: the BaFin in Germany launched an internal project in 2015 to learn more about the business model of technological Start-ups (FinTechs) and their appearance in the market. Drawing on expertise from the areas of banking, insurance and securities supervision, the objective of the project group was to observe the latest developments in the FinTech market, and to review whether BaFin needed to adjust its processes in view of new developments in the area of digitalisation. As a result of this project, BaFin established an Innovation Hub focussing on Financial Innovation Technology including, but not limited to, unregulated or start-up entities. This Innovation Hub analyses and evaluates upcoming technological solutions and new business models based on those solutions.

Additionally, the Innovation Hub coordinates a network of experts from various areas of responsibility within BaFin, which rates innovative business models with regard to regulatory requirements. Experts from the banking, insurance and securities sectors are represented in the network, but also from the directorates in charge of licensing and the pursuit of unauthorized business. The combination of experience and expertise from ongoing oversight and review of licensing requirements allows rapid assessment of innovative business models and processes that may not be unique to one sector alone.

Example: in 2016, in France, the ACPR has launched a FinTech Innovation cluster dedicated to FinTech and financial innovation. This team provides an interface between the project promoters and the ACPR directorates concerned, as well as the Banque de France (for the files relating to payment services) and the Autorité des Marchés Financiers (for files relating to investment services). The ACPR FinTech Innovation division analyzes innovations and monitors the digitalisation of French financial companies. It also provides specific support to understand the regulations and the statutes applicable to the planned activities as well as preparing the way towards an authorization/licensing process.

Example: in the UK, the regulators recognise that firms find it more difficult to enter some sectors of the financial services market than others. In banking, new entrants have in the past found it difficult to meet the high regulatory and capital requirements and the costs of implementing and maintaining branch infrastructure. Since 2016, the UK FCA and UK PRA have worked closely together to encourage competition in retail banking through the New Bank Start-up Unit. A dedicated, jointly-staffed team supports potential entrants, explaining the regulatory requirements, helping them through the authorisation process and providing support for two years after authorisation to help them adapt to the requirements.

Example: the Japan FSA amends existing regulatory policies, rules and practice as needed. For example, the Banking Act was revised in response to advances in information and communication technology and other changes in the environment, for the purpose of promoting open innovation (innovation by cooperating/working together) between financial institutions and FinTech companies while ensuring user protection.

4. Policy makers should ensure that the approach to regulation and supervision should allow new business models to operate in a way that allows them to innovate, compete and challenge established firms and business models without putting

consumers at unacceptable risk. Where relevant, policy makers should explore ways of promoting competition, enhancing interoperability and simplifying the exchange of and access to data between market.

Example: in Hong Kong, the HKMA published a revised Guideline on Authorization of Virtual Banks in May 2018, following the completion of a public consultation. Both financial firms (including existing banks) and non-financial firms (including technology companies) may apply to own and operate a virtual bank. During the period from March to May 2019, the HKMA granted banking licences to eight companies to operate in the form of a virtual bank. Virtual banks are subject to the same set of authorization criteria and supervisory requirements applicable to conventional banks, so as to ensure a level-playing field and to protect the interests of consumers. That being said, some of the supervisory requirements will be adapted to suit the business models of virtual banks under a risk-based and technology-neutral approach.

Example: in Italy, the Bank of Italy has set up a multi-disciplinary team (involving different departments of the Bank of Italy, e.g. IT, Economic Research, Payments System Oversight, Monetary Policy, Banking Supervision, Consumer Protection and anti-money laundering, Legal), in order to carry out the activities of the Innovation hub: it analyses financial innovations, monitors the market trends and encourages the development of private business initiatives, pointing out to the players how to operate in accordance with the Italian regulation. In addition, the Bank of Italy has set up a dedicated page on its website and a specific e-mail address through which operators can present, by filling and submitting a standardised application form, their financial services projects that contain innovative features.

Example: the UK FCA is carrying out a review of retail banking business models. This review looks at the core differences between emerging and traditional retail banking business models. It assesses how these differences are being driven by technological change and innovation and how they affect competition and firms' conduct. It particularly wants to understand what impact the growing use of digital channels and declining use of branches is having on business models and the implications of this for consumers.

Example: BaFin follows the "same business, same risks, same rules" principle – combined with a proportionate supervisory approach – to maintain a level playing field and ensure market stability and consumer protection. Since the regulatory framework is technology-neutral the market is open to new business models and the use of new technologies.

Example: the Central Bank of Portugal, together with the other financial supervisors (the Securities Market Commission and the Portuguese Insurance and Pension Funds Supervisory Authority) organizes and participates in the "The Portugal FinLab". This initiative constitutes a communication channel between innovators – new players in the market or incumbent institutions – and the Portuguese supervisory authorities. Through this channel, supervisors provide guidelines to the participants on how to navigate and operate in the regulatory system. The purpose of the Portugal FinLab is to support the development of innovative solutions in FinTech and related areas through cooperation and mutual understanding.

Furthermore, the Central Bank of Portugal, following a close dialogue with institutions and other market players, its monitoring process in place and horizontal assessments of the credit market through surveys (2016 questionnaire on financial institutions regarding the commercialization of banking products and services on digital channels in Portugal) identified barriers to the current account opening process through digital means. In order to remove those barriers, regulations were amended to provide for new mechanisms that, in the case of opening a bank deposit account at distance, make it possible to verify the customers' identification data, without compromising security, information transparency and the rights of bank customers.

5. Oversight bodies (i.e. domestic public authorities responsible for the oversight of financial consumer protection) should adopt a risk-based approach to digital financial products, focusing on areas of highest risk to consumers. This approach should also be flexible enough considering that technology enables firms to change their business and distribution models. Importance should be given to cybersecurity issues, as appropriate, to promote trust in digital financial products and services.

Example: in Hong Kong, the HKMA published the Open Application Programming Interface (API) Framework (Framework) for the Hong Kong banking sector. The Framework takes a risk-based principle and by phases to implement various Open API functions, and recommends prevailing international technical standards to ensure fast adoption and security. It also lays out detailed expectations on how banks should onboard and maintain relationship with third party service providers in a manner that ensures consumer protection.

Example: in 2017, the HKMA announced a number of initiatives to prepare Hong Kong to move into a New Era of Smart Banking and encourage the banking sector to embrace the opportunities brought about by the convergence of banking and technology. In particular, Banking Made Easy initiative aims to minimise regulatory frictions to promote customers' digital experience, including online wealth management. The HKMA has worked closely together with the Securities and Futures Commission (SFC) and the Insurance Authority, and promulgated risk-based regulatory standards for online wealth management.

Example: in Japan, the FSA conducts off-site and on-site monitoring with a risk-based approach to the crypto-asset broker-dealers, on the basis of the result of the risk assessment including system safety, AML/CFT and segregation of assets.

Example: in Germany, the BaFin published its circular concerning supervisory requirements for IT in the insurance sector (Versicherungaufsichtliche Anforderungen an die IT – VAIT). The VAIT are set to become the cornerstone of IT supervision for all insurance undertakings and pension funds in Germany. VAIT primarily targets the level of senior management. The objective of the VAIT is to provide the senior management of insurance undertakings with a clear and flexible framework, particularly in relation to IT resource management, information risk management and information security management, with the latter being particularly important with regard to client's personal and financial data. The VAIT are also intended to help increase

awareness of IT risks in insurance undertakings and in relation to their IT service providers. The VAIT clarify what BaFin expects from these undertakings with regard to the management and control of IT operations, including the required access rights management. In addition, the VAIT lay down the requirements for IT project management and application development, which also encompasses end-user computing in business units. Overall, the VAIT address all the issues that BaFin considers to be particularly significant based on the findings of its IT supervisory activities and inspections.

In November 2017, BaFin had already published the Supervisory Requirements for IT in Financial Institutions (Bankenaufsichtliche Anforderungen an die IT –BAIT) with a similar focus and ruleset.

Background information: The basis of insurance supervision in Germany (and the EU) is Solvency II, which follows a strictly risk-based approach and proportional approach. Among others supervisory tools, supervised insurers are required to challenge their own risks and solvency by using self-imposed adequate methods and compare the outcomes to the outcome of the standard formula. This obligation has to be fulfilled at least once a year (or in response to changes in the risk profile). Furthermore, supervised insurers can apply to calculate their solvency capital requirements via a BaFin approved internal (partial / full) model.

Example: for the Central Bank of Portugal, the oversight of the sale of consumer credit via digital channels is a top priority. Institutions are increasing the use of digital channels to sell credit to consumers and it is necessary to ensure that they comply with the comprehensive legal requirements. Maintaining a high level of consumer protection is essential to ensure consumer confidence in digital channels.

Through Circular Letter no. 4/2018, the Central Bank of Portugal required institutions that intend to offer consumer credit products or services via digital channels to provide information on their marketing whose contracting process initiates and concludes via homebanking, online platforms and mobile applications (apps). Institutions must report, at least ten business days in advance, information, such as available means to clarify customers' doubts, customer authentication procedures and security mechanisms. Additionally, supervised institutions must submit the pre-contractual information documents and the product information sheet before the scheduled date for the commencement of the provision of said product via digital channels. This information will enable the central bank to monitor and supervise the marketing of consumer credit via digital channels so as to ensure respect for the rights of bank customers, in particular in the access to pre-contractual and contractual information. The Central Bank of Portugal has also been conveying institutions they should adopt secure methods of strong customer authentication of bank clients in the access to digital channels and in the moment of expressing willingness to celebrate a credit contract.

6. Oversight bodies should cooperate when developing and applying the legal, regulatory and supervisory framework referred to digital financial consumer protection.

Example: in 2016, Spain created an inter-departmental working group with the aim of sharing information on the evolution of digital financial services

provision, ensuring financial stability, financial consumer protection, the promotion of competitiveness among final services providers, and the identification of areas that require decision-making or adoption of measures by competent authorities. This working group comprises representatives of the different public authorities with competences in relation to the regulation (Ministry of the Treasury) and supervision of financial institutions in Spain (Banco de España - banking sector; CNMV - securities sector; and DGSYFP - insurance sector).

In meeting and consulting with non-governmental stakeholders, policy makers can use opportunities to gather and share information about risks, trends and challenges posed by technological developments, set out thinking, lead or contribute to the debate on emerging topics, or raise awareness of particular issues.

Example: in 2016, South Africa established the Intergovernmental FinTech Working Group (IFWG). It comprises members from National Treasury, the South African Reserve Bank, the Financial Sector Conduct Authority and the Financial Intelligence Centre, and was formed to develop a common understanding among regulators and policy makers of fintech developments and policy and regulatory implications for the financial sector and economy. In April 2018, the IFWG hosted its inaugural workshop to engage with industry on key considerations, including risks and benefits involved in financial services innovation driven by technology, the regulatory challenges faced by fintechs in South Africa, and the response that regulators should take to develop appropriate policies and implement effective regulatory frameworks for this emerging industry. The workshop was attended by fintech firms, incumbent financial institutions, academic institutions, regulators and policy makers, and other stakeholders. A report on the discussions and outcomes of the workshop was produced and distributed[2], and it is anticipated that the IFWG will host these workshops on a regular basis.

Example: in Italy, a Committee on automation in the banking industry has been long established by joint initiative from the Bank of Italy and the Italian Banking Association; participation to the Committee is allowed, among others, to banks and companies running relevant financial infrastructures. While the Committee is especially involved in the development of initiatives aimed at increasing the overall efficiency of the financial system and the smooth interaction among its components, a relevant stream of work is represented by the Yearly Review on the state of Automation in the Italian banking sector. Furthermore, the Committee has recently devoted research efforts to how a highly digitised environment affects the banking sector: in 2019, a report was released on the issue of Open Banking; in 2018, a report was published on the impact on banks of technological innovation and artificial intelligence.

Since 2014, the Bank of Italy has held meetings with association of consumers at least twice a year, in order to discuss issues relating to financial consumer protection and gather information about emerging trends and risks as they are perceived by consumers. Meetings with industry representatives are held in relation to major supervisory actions (e.g. before issuing Guidelines on

[2] http://www.treasury.gov.za/publications/other/IFWG%20Report%20April%202018.pdf

consumer protection related topics) in order to gather information on the feasibility of the supervisory expectations to be outlined and also to make them aware of supervisory expectations.

Example: in April 2018, BaFin hosted the "BaFin-Tech 2018" conference and discussed the consequences of digitization and financial technology innovations with about 400 representatives of new and established companies in the financial industry as well as experts from supervision and academia. The third edition of the BaFin Tech has taken place in September 2019 featuring topics like Blockchain and Artificial Intelligence and corresponding business models.

Additionally, the digitization efforts of the German insurance sector was one of the key topics of the annual Insurance Supervision Conference 2017 and 2018, providing the opportunity to share the supervisory perspective with stakeholders from the insurance sector and allowing discussions amongst all participants.

Moreover, in June 2018 BaFin published a report on the challenges and implications arising from the use of Big Data and Artificial Intelligence (BDAI) in the financial sector. The launch of the report was accompanied by a call for consultation, particularly from non-governmental stakeholders, on the key questions raised in the report.

Example: in France, the *Forum FinTech*, launched by the ACPR and the AMF, brings together innovative firms, public authorities and supervisors, in order to better understand challenges linked to the development of fintechs. It can be consulted on all regulation projects and can formulate recommendations.

Example: the Central Bank of Ireland's Consumer Protection Directorate (CPD) meets with key industry and consumer representative bodies on a regular basis. The Consumer Protection Directorate also benefits from the advice of the Consumer Advisory Group ('CAG'), which consists of a number of experts, who provides views on initiatives aimed at further enhancing the protection of consumers of financial services in Ireland. The CAG also comments on documents, consultation papers or other materials prepared by the Central Bank's staff. CPD organises two 'roadshows' per calendar year. These events afford Retail Intermediary Firms and related representative bodies an opportunity to meet with members of CPD's Supervisory Team. CPD staff present on a number of topics (including On-going Regulatory Matters, Anti-Money laundering, Cyber Risk and IT and Industry Funding Levy). The roadshows are attended by ca. 500 people and are held in different locations each year. In arranging these Roadshows, CPD hears first-hand from the intermediary sector the concerns they have around certain policy proposals under consideration by the Central Bank (such as inducements/commissions paid to intermediaries and the digitalisation of financial services).

Example: the UK FCA publishes Occasional Papers on key issues to broaden understanding, stimulate interest and debate as well as offer practical help to firms. Since 2015 it has published occasional papers on both consumer vulnerability and access to financial services. The vulnerability occasional paper was accompanied by a practitioners pack. This has supported UK trade bodies to develop or review vulnerability strategies in their sectors. Its access

to financial services in the UK occasional paper was authored by leading academics alongside FCA experts. Rather than presenting a definitive FCA view, the FCA intended it to prompt debate by bringing together the key issues of consumer access. It has followed up these papers in its supervisory discussions with firms.

Example: the Central Bank of Portugal cooperates with the other financial supervisors (The Securities Market Commission and the Portuguese Insurance and Pension Funds Supervisory Authority) within the "The Portugal FinLab". With a coordinated approach promoted by the National Council of Financial Supervisors (*Conselho Nacional de Supervisores Financeiros*) – established to enhance coordination and articulation among financial supervisory authorities – Portuguese financial supervisors are brought together around this innovation hub, providing innovators (start-ups or incumbents) with all the needed information to navigate and operate in the regulatory system.

Example: in 2010, amendments to legislation expanded the Financial Consumer Agency of Canada's (FCAC) role to increase its ability to undertake research, field testing and stakeholder engagement to provide information to the government on financial consumer trends and emerging issues. As part of FCAC's strategic imperatives, the Commissioner has made the identification of trends and emerging issues that impact consumers a priority and has committed to engage and consult on financial consumer protection issues.

To support this effort, the Consumer Protection Advisory Committee (CPAC) was established to engage and consult a wide range of stakeholders on financial consumer protection issues. CPAC is a forum of public, private and non-profit organizations, as well as individual experts, with the following objectives:

- Provide information on financial consumer protection issues in support of FCAC's financial consumer protection mandate
- Identify and evaluate trends and emerging issues of relevance to financial consumers
- Share and discuss research relevant to FCAC's financial consumer protection mandate and identify research opportunities
- Bring to bear all of its knowledge and expertise in the best interests of financial consumers

FCAC's Financial Literacy initiatives work to strengthen the financial well-being of Canadians and their families. This includes valuable resources and initiatives such as:

- organizing a National Conference on Financial Literacy
- providing free programs, tools and resources to help employers offer financial education in their workplace
- designing educational materials for all to use
- developing financial tools and calculators, including budget and mortgage calculators and tools to help choose a bank account and/or credit card

- maintaining the Canadian Financial Literacy database – a source for resources and events from Canadian organizations on budgeting, saving, investing and more

FCAC also undertakes Industry Reviews as a way of gathering information from multiple regulated entities or stakeholders on specific market conduct matters and on matters related to the financial services sector generally. These reviews serve to achieve any of the following objectives:

- to assess current or emerging issues on a specific topic or theme
- to identify and examine industry practices or trends
- to verify levels of compliance with market conduct obligations
- to collect information for policy discussions

7. Oversight bodies should consider ways of communicating directly with consumers about relevant digital financial consumer protection issues for example emerging risks with new products or distribution channels. This can be done, for example, using mass media channels (e.g. websites, traditional and social media, publishing informative, explanatory and awareness documents), organising conferences or town hall meetings etc.

> Example: the HKMA conducts Consumer Education Programme to promote "smart & responsible" use of banking and financial services, including ATMs, internet banking, mobile banking, and other digital financial services such as using bank smartphone apps in conducting peer-to-peer fund transfers, and raising the public awareness of the HKMA's new initiatives such as the new payment financial infrastructure "Faster Payment System" launched in September 2018 that facilitates instant cross-bank and e-wallet money transfer anytime, anywhere. Tips on enhancing the public's cybersecurity awareness and knowledge on using such services are promoted on an on-going basis. Packaged in form of video and audio clips, comics and leaflets, the tips are disseminated via TV, popular websites and smartphone apps (including the HKMA website and YouTube Channel), radio, print media, cinemas, public transport, HKMA Information Centre and Coin Carts and roving exhibitions at high-patronage shopping malls. The HKMA also promulgates the tips to secondary and tertiary students in its youth education activities such as online quiz and talks.

> Example: in conjunction with major supervisory initiatives, the Bank of Italy has addressed warnings to consumers to raise awareness on issues that are relevant for them. The Bank of Italy website also provides consumers with information on banking products and services and interactive tools to preliminarily assess the potential suitability of the products and services. In order to increase consumer understanding, the Bank of Italy publishes on its website "Guides" about different products; the goal is to help consumers to understand the characteristics of financial products, in order to make informed choices by comparing different available offers and to know where to go for assistance. Banks and other financial institutions are requested to make the Guides available on their website.

The Bank of Italy also has a newsletter on consumer protection issues, which is a communication channel with the public, aiming at providing news and tips for the benefit of financial services clients about consumer protection.

Example: in Germany, BaFin runs a special, free-of-charge consumer helpline. The helpline staff answer consumers' questions or explain the measures available if consumers want to settle a conflict out of court with financial service entities. As a special service there is a sign language phone service for the deaf and people with hearing difficulties. The consumer helpline offers also "co-browsing", a feature that allows consumer helpline advisers to navigate to websites together with callers. In addition, BaFin publishes a monthly journal (BaFin Journal) with i.e. articles directed to consumers. The journal is publicly available on the BaFin website.

Besides this regular format BaFin also publishes brochures for people with learning difficulties (e.g. "Investment Alphabet").[3] In cooperation with an organization for elderly citizens BaFin organizes the so-called "digital regulars' table". This event has the shape of a Skype conference, allowing consumers – in this case elderly people – to address their questions directly to BaFin experts. BaFin also publishes online warnings about specific products or types of products.[4]

Example: The Banque de France, the ACPR and AMF have a joint dedicated website (https://www.abe-infoservice.fr/) for communicating directly with consumers. The website provides practical information on banking products, insurance and financial investments; provides guidance to consumers in their efforts before the completion of a transaction or when they wish to make a complaint; helps the public to protect themselves from scams; provides alerts on unauthorized practices, actors or websites; and collects information or complaints that customers wish to bring to the attention of the authorities. The website uses a diverse range of communication media: news, informative articles in the form of Q&As, alerts, videos and newsletter.

In 2017, the Banque de France launched "The Lab". As an open space for discussions and collaborative work, the Lab links up the Banque de France with various initiators of innovative projects - start-ups and fintechs, institutional players, universities - in order to experiment with new concepts and technologies in connection with the activities of the institution. The Lab is working on technologies such as blockchain (MADRE project), IoT, IA etc.

Example: the Central Bank of Ireland issues a press release and/or tweets about any new publication. It also uses social media to both encourage and remind stakeholders – including members of the public to comment on discussion and consultation papers that are on the Central Bank's website. The Central Bank of Ireland's recently revamped website contains a consumer-focused section, known as the "consumer hub" (see: https://www.centralbank.ie/consumer-hub) where some key aspects of the Central Bank's work are explained using plain English and infographics, which are aimed at explaining new rules in a simple/plain English manner. This part of the website also contains videos of

[3] https://www.bafin.de/SharedDocs/Downloads/DE/Broschuere/dl_b_geldanlage_leichte_sprache.html

[4] https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Meldung/2017/meldung_171109_ICOs.html

interviews with staff explaining a particular policy proposal, new initiative or supervisory action, as well as a FAQ section and a number of (downloadable) consumer guides.

The Central Bank also has a dedicated Public Contacts Unit, which responds to queries from members of the public and manages the Central Bank's Visitor Centre. The Central Bank of Ireland is also involved in a number of community outreach projects and school initiatives. In an effort to reach the largest possible audience, the Central Bank actively participates in other public or societal events such as graduate fairs, Culture Night, Open House and the annual Ploughing Championships.

Example: the Central Bank of Portugal, through its Bank Customer Website (https://clientebancario.bportugal.pt/en/) provides information to bank customers and regularly issues publications on subjects related to retail banking products and services, including those related to the commercialization through digital channels (e.g. how a banking consumer should protect itself against on-line fraud). In this website it has been published videos and explainers, namely on mortgage credit and payment services.

Through the Bank Customer Website, the central bank has also been promoting awareness campaigns. As an example, in 2018 it was launched the digital financial education plan with a view to stimulate a safe use of digital channels. Furthermore, in September 2018, the Central Bank of Portugal launched a digital financial education campaign for young people (#toptip), aiming at raising awareness among school-age children of precautions to take when using digital channels to access banking products and services. Within this campaign, five messages over five weeks on five different topics were disseminated ("When you use the internet do you have any idea of the risks?", "Do you use your phone (smartphone) to access social networks or email? And homebanking? Do you also make payments with your phone?", "Is social media your second home?", "Is social media your second home?", "What if you are a victim of online fraud?"). Within this campaign, the Central Bank of Portugal prepared a brochure and conducts financial education initiatives in schools throughout the country.

Example: Japan FSA issued information and a warning on crypto-asset and ICO such as its trend or price fluctuations at the FSA website, targeting both users and business operators. For example, in August 2018, the FSA published the interim reports of on-site and off-site inspections/monitoring for crypto-asset broker-dealers which were conducted by the FSA so far, which shows key findings from the inspections and monitoring.

Example: Banco de España has increased its effort in approaching the consumer through its website (Banking Client Portal (https://clientebancario.bde.es/pcb/en/) and other initiatives aimed at bringing the financial world closer to the consumer, like collaborating in promoting financial education.

Example: FCAC develops educational content for consumers related to financial products and services, including specific material related to consumer rights and responsibilities. In addition, FCAC publishes timely consumer alerts as new issues requiring immediate consumer attention arise.

FCAC can reach consumers through a range of platforms with the use of traditional and social media channels. Consumer summits organized through FCAC provides another venue to promote the work of the Agency as a result of research, industry reviews, and other initiatives.

Principle 2: Role of Oversight Bodies

There should be oversight bodies (dedicated or not) explicitly responsible for financial consumer protection, with the necessary authority to fulfil their mandates. They require clear and objectively defined responsibilities and appropriate governance; operational independence; accountability for their activities; adequate powers; resources and capabilities; defined and transparent enforcement framework and clear and consistent regulatory processes.

Oversight bodies should observe high professional standards, including appropriate standards of confidentiality of consumer and proprietary information and the avoidance of conflicts of interest.

Co-operation with other financial services oversight authorities and between authorities or departments in charge of sectoral issues should be promoted. A level playing field across financial services should be encouraged as appropriate.

International co-operation between oversight bodies should also be encouraged, while specific attention should be considered for consumer protection issues arising from international transactions and cross-border marketing and sales.

8. Oversight bodies should ensure they have adequate knowledge of the financial services market. They may do this by:

- conducting market reviews or research to understand developments e.g. in terms of new products or services, distribution channels and providers.

Example: in December 2016, the Bank of Portugal launched the first 'Questionnaire on banking products and services through digital channels' in order to assess the development of digital financial services in Portugal, the levels of adoption and use by customers, the constraints and obstacles to the demand for digital channels, and the main risks associated with the provision of financial services through digital channels. The results of this questionnaire were presented in the 2016 Banking Conduct Supervision Report and in a brochure about the financial products and services provided through digital channels in Portugal. (https://clientebancario.bportugal.pt/ sites/default/files/relacionados/publicacoes/QuestCanaisDigitais2016_EN.pdf)

Example: the Bank of Italy in 2017 conducted research on a sample of the most representative national financial intermediaries it supervised. The results were presented in the report Fintech in Italia (www.bancaditalia.it/compiti/vigilanza/analisi-sistema/stat-bancheintermediari/Fintech_in_Italia_2017.pdf)

- engaging proactively and regularly with businesses (both existing and new) regarding innovative products, services or channels.

Example: in 2016, the Federal Financial Supervisory Authority of Germany (BaFin) hosted the first conference called BaFin-Tech which brings together representatives of young businesses and FinTech companies as well as established financial services providers, industry associations, the German regulator (Federal Ministry of Finance) and the German supervisor (BaFin). This event facilitated the exchange of experiences and allowed for discussions about new developments in this area. In April 2018, the second edition of the BaFin-Tech took place dealing with such topics as Big Data, Artificial Intelligence, Initial Coin Offerings, Blockchain, Cloud

Computing and RegTech. The third edition took place in September 2019 with a focus on Blockchain and Artificial Intelligence and corresponding business models.

Additionally, BaFin hosts on an annual basis the Insurance Supervision Conference providing the opportunity to share the supervisory perspective with stakeholders from the insurance sector (incumbents and Tech firms). The digitization efforts of the German insurance sector was one of the key topics of the annual Insurance Supervision Conference 2017 and 2018. In 2019 the key note speech will be on the admission and ongoing supervision of Insurtechs in times of digital transformation.

Example: in November 2017, the Bank of Portugal hosted the event "Paychallenge': The Future of Payments and Fintech" bringing together the national supervisor, financial institutions, startups/ FinTech companies, representatives of the Government and the European Commission. This event intended to discuss and promote innovative solutions for payment services, taking into account the PSD2. In February 2018, the Bank of Portugal also organized an internal conference ("Digital to the Core: The importance of new technological platforms for Digital Disruption in organisations") with representatives of financial services providers with expertise on artificial intelligence, big data, blockchain, digital authentication and RegTech. The purpose of this event was to exchange views and experiences and to identify best practices, new and emerging strategies.

- engaging with industry representatives and other relevant stakeholders to get information in relation to technological developments and trends and emerging issues in the market, including in converging and connected markets. Such issues may include the preparedness for dealing with cyber incidents.

Example: the Japan Financial Services Agency (JFSA) has encouraged financial institutions to enhance their management of cyber-security through monitoring their management system. In October 2018, the JFSA issued the updated Policy Approaches to Strengthen Cyber Security in the Financial Sector to address new challenges, in particular:

1. Responses to accelerating digitalization
2. Contribution and responses to international discussion
3. Responses to Tokyo Olympic and Paralympic Games in 2020.

In June 2019, The JFSA published the Financial Sector Cybersecurity Report that mainly reflects the current state and common issues of cyber security across the financial sector ascertained in the program year 2018, based on the JFSA's Policy Approaches to Strengthen Cyber Security in the Financial Sector. The key points of the report is as follows,

- Identify and analyze the impact of digitalization on financial sector, cyber-security-related risks and countermeasures, etc. through interviews with IT vendors, large financial institutions, etc.
- Participated in the G7 joint cross-border crisis management exercise on cyber incident to enhance coordination among G7 financial authorities for responding to cyber incidents affecting the global financial system
- Work with industry groups in the financial sector to establish the "Liaison Council for Cybersecurity Stakeholders" to enable information to be shared when cyber incidents, particularly major incidents, occur (June 2019)

- Conducting FSA cybersecurity exercises (DeltaWall III) (October 2018) to strengthen cyber-security measures including the preparedness for dealing with cyber incidents.
- engaging proactively and regularly with consumers, including conducting consumer research, and with consumer representatives to ensure an adequate understanding of the issues and experiences from the perspective of consumers in relation to digital financial services.

Example: in November 2019, the Federal Financial Supervisory Authority of Germany (BaFin) will host the sixth edition of the Verbraucherschutzforum (Consumer Protection Forum). This time the focus will be on consumer protection in the financial market in the age of digitization and sustainability. Questions such as ″Are we protecting or patronizing the consumer?″ will be discussed. Lectures, panel discussions and a workshop address the current requirements for consumers as well as the underlying notion of "consumer". The event is aimed at consumer protection organizations, associations, the financial sector, science and politics.

Example: in 2018, the Financial Consumer Agency of Canada (FCAC) established the Consumer Protection Advisory Committee (CPAC). Through CPAC, FCAC will broaden stakeholder engagement beyond traditional players. This will enhance the Agency's capacity to identify and respond to emerging financial consumer protection issues, while providing an important avenue for stakeholders to voice concerns and provide feedback on related issues, including digital financial services. Its members will help inform supervision activities, research initiatives, consumer education material and provide important input on evolving consumer needs.

- engaging with other relevant financial and non-financial oversight bodies to ensure market developments and key trends are communicated, facilitate information sharing or coordinated monitoring activities in areas of mutual interest.

Example: in May 2020, the Federal Financial Supervisory Authority of Germany (BaFin) will host its first international supervisory forum on consumer protection. This conference will bring together representatives of the financial regulatory and supervisory community to engage in discussing the latest developments in consumer protection and finding common solutions to identified challenges. This event plans to focus on issues such as risks and chances of digitalisation in consumer protection, identifying alternatives to disclosure, defining the notion of "consumer", or the role of gamification in consumer education.

9. Oversight bodies should ensure existing regulatory and supervisory tools and methods are adapted to, and explore new avenues for operating effectively in, the digital environment. Actions could include:

- establishing or upgrading systems and processes to collect, store and analyse relevant data to inform regulatory decisions and supervisory efforts and understand the behaviour of market participants, including consumers.

Example: through the establishment of an Analytics Centre of Excellence, the United Kingdom Financial Conduct Authority is exploring how innovative technology and techniques, including artificial intelligence and machine learning, can be applied internally by regulators. The FCA is looking at how these approaches can, for example, enable the automation of the manual processes, allow the adoption

of population review rather than sampling, and support the development of better predictive analytical models of potential harm.

- ensuring access to, or being able to gain access to, such data as is necessary to allow for effective off-site monitoring.

Example: in Germany, BaFin has the authority to request any set of data or information from supervised entities. Also, there are numerous regular reporting obligations, by which BaFin receives data on market transactions, majority shifts in shares of exchange traded companies, or data relevant to the identification of fraud, money laundering or market manipulation. BaFin constantly works on ways to effectively analyse and process this data and to identify fitting regulatory or oversight responses to eventual findings.

- exploring the use and application of technology (i.e. RegTech or SupTech) to assist them to supervise financial services providers and identify and monitor risks arising in the financial system.

Example: in conjunction with the Bank of England and market participants, the United Kingdom Financial Conduct Authority has recently developed a 'proof of concept' to make a regulatory reporting requirement machine-readable and executable. This means that firms would be able to map reporting requirements directly to the data that they hold, creating the potential for automated, straight-through processing of regulatory returns. For regulators, this creates the potential for more consistent and granular data collection, the more efficient identification and monitoring of issues, and earlier diagnosis of harm and potential intervention. The FCA has recently published a Call for Input to further develop this idea.

Example: the Hong Kong Monetary Authority has launched a series of RegTech-specific projects in September 2018 to facilitate the adoption of RegTech in Hong Kong, focusing on anti-money laundering/counter-financing of terrorism (AML/CFT) surveillance technologies; RegTech for prudential risk management and compliance; and a study on machine-readable regulations.

10. Oversight bodies have the right resources and capabilities to operate effectively and flexibly in the digital environment, for example by:

- ensuring that their staff have the right mix of skills and capabilities to identify and understand potential risks arising from the design and distribution of digital financial services.
- ensuring staff training and development is up to date with latest technological developments and applications.

Example: the Central Bank of Ireland has set up an internal Fintech Group to look at technological innovation across the range of sectors and activities, and seek to ensure that the Central Bank has a holistic view of those developments and how the Central Bank responds to them. This work has been carried out both by drawing on the Central Bank's in-house knowledge but also by engaging with industry and commercial providers, including start-ups and incumbents, and support providers such as incubators and accelerators.

11. Oversight bodies should be capable of dealing with technological innovation issues and developments in an effective and multidisciplinary way, while ensuring key consumer protections are maintained. In relation to licensing or authorisation

requirements, this can be done by establishing mechanisms or adopting proportionate approaches which allow businesses to be innovative, while maintaining relevant safeguards and protection.[5]

Mechanisms may include for example establishing "regulatory sandboxes" or "innovation hubs". Where regulatory sandboxes or other testing methods are established, they should be governed by clear rules or principles to ensure fairness, transparency, consumer protection and open access to existing and new market participants.

Other approaches are possible, such as proportionate regulatory approaches and/or the provision of regulatory support to promote better understanding of existing regulations from the outset and therefore improve their ability to comply.

> Example: the United Kingdom Financial Conduct Authority operates a Regulatory Sandbox, which allows established businesses and start-ups test innovative propositions in the marketplace, ensuring appropriate consumer safeguards are in place.
>
> Example: the CSSF in Luxembourg has imposed additional disclosure requirements on supervised entities, such as warnings about the specific risks of products or services.
>
> Example: the Hong Kong Monetary Authority launched the Fintech Supervisory Sandbox (FSS) in September 2016, which allows banks and their partnering tech firms to conduct pilot trials of their fintech initiatives without the need to achieve full compliance with the HKMA's supervisory requirements during the trial period. The FSS enables banks and tech firms to gather data and user feedback earlier so that they can make refinements to their new initiatives, thereby expediting the launch of new technology products, and reducing the development cost.
>
> Example: Spain is developing a sandbox law in order to promote fintech projects. This initiative will allow the creation of a flexible and controlled (but not "unregulated") space to test different innovative projects. It seeks to support innovation and will also serve as a learning tool for regulators.
>
> Example: in France, the AMF has created a "coach system" consisting of regulatory support for new entrants, which leads to a better understanding and adoption of the applicable regulations, and avoids non-compliant business models developing.
>
> Example: in Germany, BaFin launched an internal project in 2015 to learn more about the business model of technological Start-ups (FinTechs) and their appearance in the market. Drawing on expertise from the areas of banking, insurance and securities supervision, the objective of the project group was to observe the latest developments in the FinTech market, and to review whether BaFin needed to adjust its processes in view of new developments in the area of digitalisation. As a result of this project, BaFin established an Innovation

[5] Examples of such approaches could include granting conditional or time-limited authorisations/licences, setting investment limits, imposing additional disclosure requirements or establishing expedient internal dispute resolution systems, are examples of tools that oversight bodies may use in allowing new approaches to be tested.

Hub focussing on Financial Innovation Technology including, but not limited to, unregulated or start-up entities. This Innovation Hub analyses and evaluates upcoming technological solutions and new business models based on those solutions.

Additionally, the Innovation Hub coordinates a network of experts from various areas of responsibility within BaFin, which rates innovative business models with regard to regulatory requirements. Experts from the banking, insurance and securities sectors are represented in the network, and also experts from the directorates in charge of licensing and the prosecution of unauthorized business. The combination of experience and expertise from ongoing oversight and review of licensing requirements allows rapid assessment of innovative business models and processes that may not be unique to one sector alone.

12. Creating internal working groups to deal with innovation issues (responding to requests for information from businesses, evaluating compliance with the existing legal and regulatory framework for new products and services, etc.) with the participation of relevant units/departments and, where relevant, oversight bodies responsible for data protection and competition.

Example: the Bank of Portugal set up an internal and multidisciplinary working group to respond to the challenges of the digital banking and FinTech, promoting reflection, in the context of the Portuguese financial system within its Strategic Plan 2017-20. This group is composed of representatives of different areas of the Central Bank – for example, micro-prudential, macro-prudential and banking conduct supervision, payment oversight, technology and monetary policy – and is chaired by a member of the Board of Directors.

Example: in November 2017, the Bank of Italy set up an internal, multi-disciplinary working group on fintech and recently launched a new "Fintech Channel". The objective of this Channel is to support innovation processes in the regulatory arena, adopting a forward-looking approach. Applications from startups and firms that would propose to offer technological solutions to banks and financial intermediaries, or the latter if they are directly involved in the development of innovative solutions in the area, submitted via a dedicated email address undergo multifunctional screening tailored to each situation. In the course of the review, operators are given feedback through meetings and telephone calls, for example.

Example: the CSSF in Luxembourg has created a working group comprising CSSF staff and external experts, in order to take a proactive approach to fintech developments. The objective of the group is to examine innovation, to define whether specific innovations would be an opportunity for the financial sector and to prepare CSSF staff to assess innovative business models by defining the benefits such innovations may deliver and identifying the potential risks.

Example: in 2015, the Federal Financial Supervisory Authority of Germany (BaFin) set up an internal task force to deal with the issues arising through the phenomenon of FinTech and digitalisation. The task force comprised representatives from the banking, insurance and securities department as well as staff from several other departments concerned (e.g. IT, International Policy, Strategy and Risk, Authorisation Requirement and Enforcement). The aim of this task force was to keep up with the pace of the newest innovations and to

foster regular exchange of information. Another aspect was to consider how to facilitate the licensing process for new businesses and to easily get into contact with BaFin regarding licensing questions, while at the same time always keeping track of the supervisory principle "same business, same risk, same rules". As a result of this project BaFin established an Innovation Hub. This Innovation Hub analyses and evaluates upcoming technological solutions and new business models based on those solutions.

13. Providing advice or guidance to new entrants to the market about the application of the regulatory framework to innovative approaches or business models that may deliver benefits to consumers. Such advice or guidance could include lessons learned from dealing with innovative approaches e.g. via a regulatory sandbox. General guidance to all market participants can also be useful.

Example: the United Kingdom Financial Conduct Authority operates an Advice Unit, which provides regulatory feedback, including individual guidance, informal steers and signposting to existing rules/guidance to firms developing automated models of lower cost financial advice to consumers.

Example: the CSSF in Luxembourg provides advice or guidance to new entrants to the market about the application of the regulatory framework to innovative approaches or business models that may deliver benefits to consumers.

Example: one outcome of the task force of the Federal Financial Supervisory Authority of Germany (BaFin), was the development of a contact form for company start-ups and fintech companies who can now easily get into contact with BaFin regarding their licensing questions. On this webpage there is a self-assessment facility to get an indication about the whether it may be necessary to apply for registration for the proposed business model y (https://www.bafin.de/dok/8054672).

Example: the Japan Financial Services Agency supports fintech firms through a Fintech Support Desk and a FinTech PoC (proof of concept) Hub. The Fintech Support Desk responds to inquiries, mainly on the interpretation of the law, within 5 working days on average to address the concerns of fintech firms. The FinTech PoC Hub offers a venue for conducting trials with other relevant authorities, by forming special working teams within the FSA for each selected PoC project.

Example: the Hong Kong Monetary Authority established a Fintech Supervisory Chatroom in 2017, which seeks to provide supervisory feedback to banks and tech firms at an early stage when new technology applications are being contemplated, thereby reducing abortive work and expediting the rollout of new technology applications.

Example: in March 2018, the Treasury of Spain joined Alastria, which is the first non-profit multi-sector consortium, promoted by companies and institutions for the establishment of a blockchain/DLT semi-public infrastructure, which supports legally effective services in Spain and in accordance with European regulations. In this project, more than 200 companies have come together to create a "blockchain" platform on which applications were generated according to the legal framework. It allows associates to experience these technologies in a cooperate environment.

14. Existing regulations are evaluated and if needed redesigned, adapted or clarified.

Example: the Bank of Portugal introduced changes to the existing regulatory framework to facilitate the opening of bank deposit accounts via digital channels (online and mobile). Technical requirements for verifying customers' identification data applying to the use of videoconference were established, taking into account security and anti-money laundering concerns. The new regulations aim to facilitate the provision of digital banking products and services, to follow bank customers' new expectations and trends, and to ensure a level playing field between credit institutions with head offices or branches in Portugal and those with head offices in other EU countries. (www.bportugal.pt/en/comunicado/bancode-portugal-approves-opening-bank-deposit-accounts-video-conference-exclusively).

Example: in November 2018, BaFin published guidance considering the use of cloud computing providers in order to provide clarity on the legal interpretation of existing outsourcing requirements related to the use of cloud computing. BaFin also regularly publishes supervisory advice for consumers and financial service providers via the monthly "BaFin Journal". Each advice covers specific topics, such as robo-advisory or crypto-assets.

Example: following responses from market participants especially from the fintech sector, the CSSF in Luxembourg has published an FAQ explaining the conditions under which video identification is acceptable.

Example: the Central Bank of Ireland published a Discussion Paper in June 2017 on the Consumer Protection Code and the Digitalisation of Financial Services. The purpose of this discussion paper was to generate discussion and stimulate debate with stakeholders, on whether the current Consumer Protection Code ("the Code") adequately protects consumers in an increasingly digitalised financial services environment. The Discussion Paper focussed on specific areas of the Code which the Bank sees as being most impacted by digitalisation and technological advances: (a) access; (b) provision of information/disclosure requirements; (c) suitability; (d) complaints handling/redress; (e) claims handling process and (f) retention of consumer records/record keeping. The Discussion Paper then concludes by inviting views on whether further enhancements to consumer protection rules in the identified areas of the Code are required to ensure that innovation in financial services is always underpinned by a strong consumer-focused culture and good product oversight and governance. It is envisaged that any specific policy proposals arising from feedback given in response to this discussion paper, will be subject to consultation later in 2018/2019.

Example: the Hong Kong Monetary Authority has established a Task Force within the HKMA, under the Banking Made Easy initiative, to work with the banking industry to minimise regulatory frictions in customers' digital experience, including remote account on-boarding and maintenance, online finance and online wealth management.

Example: the Central Bank of Brazil is discussing the regulation of fintech lending. The proposed regulation aims to establish criteria for the creation and operation of two new types of financial institutions:

- SCD: this type of financial institution will operate exclusively with its own capital;
- SEP: this type of financial institution will operate exclusively with third-party capital, connecting lenders and borrowers (peer to peer lending).

These new institutions will be specialized in performing loans operations via electronic. Additionally, they will be allowed to provide a set of limited services related to the credit operation such as credit analysis and collection. In terms of financial system regulation, these institutions will follow a simplified licensing process as well as a proportional regulation according to their size and risk profile. Moreover, this regulation may increase the legal security of contracts and may contribute to the enhancement of efficiency and competition in the credit market. The Central Bank of Brazil also has introduced changes to the existing regulatory framework to allow for account opening exclusively via digital channels (online and mobile).

Example: as a follow-up to its Retail Financial Services Action Plan, the European Commission has set up an expert group to provide advice to the Commission on remote digital onboarding, a process whereby customers based in one EU Member State are able to have their electronic identification accepted remotely in order to open a bank account online in another Member State, while meeting the strong requirements for customer identity proofing and verification for know-your-customer and customer due diligence purposes.

15. The provision of financial services through digital channels can facilitate cross-border transactions which can present particular risks, e.g. in terms of the ability to seek redress or take enforcement action if required. Given this, oversight bodies from different jurisdictions should cooperate to ensure that consumers remain adequately protected. They can do this by:

- sharing information with the oversight bodies from different jurisdictions and relevant for an effective supervision of cross-border marketing and sale of financial products and services.
- where possible, ensuring that consumers' complaints in relation to cross-border transactions are redirected to the relevant competent authority.
- co-operating, for example, via international standard setter bodies, in order to promote consistency, avoid opportunities for regulatory arbitrage and support enforcement activity.[6]

Example: oversight bodies in the EU, including German BaFin, participate in the "Consumer Protection Cooperation"-Network (CPC) on the grounds of the CPC-Directive. This Directive and the corresponding national legislation enable cross-border-cooperation of oversight bodies in cases where certain services or products violate consumer rights in a multitude of Member States. The cooperation facilitates

[6] For example, securities regulators cooperate cross-border via the IOSCO Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and the Exchange of Information (IOSCO MMoU, 2002), to exchange information and assist each other for the purpose of enforcing and securing compliance with securities laws and regulations. The Joint Committee of the three European Supervisory Authorities is also working on cross-border supervision in order to increase cooperation among supervisors in Europe.

prosecution in such cross-border cases and makes it possible to impose coordinated measures and sanctions on the violator throughout the EU.

Principle 3: Equitable and Fair Treatment of Customers

All financial consumers should be treated equally, honestly and fairly at all stages of their relationship with financial service providers. Treating consumers fairly should be an integral part of the good governance and corporate culture of all financial services providers and authorised agents. Special attention should be dedicated to the needs of vulnerable groups.

16. Policy makers should seek to understand and where appropriate address the issues hindering consumers, particularly consumers who may be vulnerable, from fairly accessing different financial markets, products and services.

Example: in Hong Kong, to enhance the accessibility of banking services by customers with physical disabilities, visual impairment or hearing impairment, the HKMA facilitated the Hong Kong Association of Banks to issue the Practical Guideline on Barrier-free Banking Services ("Practical Guideline") in 2018. The Practical Guideline sets out the good barrier-free practices recommended for the industry with respect to all banking service channels. Examples of good practices include encouraging retail banks to set up more voice navigation automated teller machines; adoption of internationally recognized web accessibility guidelines for online banking channels; and provision of information on barrier-free banking facilitates on banks' websites or mobile apps to facilitate people with disabilities to access different banking services. At the encouragement of the HKMA, banks have also flexibly and pragmatically utilised technologies and operation modes, such as mobile branches and video teller machines, to put the spirit of financial inclusion into practice when developing their banking networks to enhance accessibility of basic banking services at public housing estates and remote areas.

Example: since the introduction of the German Payment Accounts Act (Zahlungskontengesetz – ZKG; part of implementation of European Payment Accounts Directive – 2014/92/EU), all consumers legally residing in the European Union are entitled to a basic payment account. A basic payment account can be used like a current account but is subject to certain protective restrictions, especially regarding installation and termination of the account. All consumers legally residing in the European Union are entitled to conclude a contract for a basic payment account, without a possibility of rejection by the bank. This also applies to persons without a permanent place of residence, asylum seekers and persons without a residence permit who cannot be deported due to legal or factual reasons.

The German General Equal Treatment Act prohibits different treatments based on religion, disability, age or sexual identity in private insurances except where these differences base on approved principles of risk-adequate calculation, i.e. an actuarial risk assessment using statistical surveys to protect consumers from arbitrary acts. Additionally, the principle of equal treatment is a legal requirement for certain insurance schemes stating that all factors being equal, the same principles must be used to calculate premiums and benefits.

Example: in France, the question of vulnerable consumers is one of the ACPR' business practice supervisory priorities. The aim is to shed light on what underlies the notion of vulnerability, and the consequences in terms of regulation or supervision. The work is conducted by a dedicated working group

comprising representatives of the ACPR and of the Financial Markets Authority (AMF). After a study dedicated to "protected adults" in 2016 and 2017, ACPR started a new study on ageing populations. The goal is to know more about the nature and quality of relationships between the elderly and financial institutions, and how the latter manage this specific clientele. The project is divided into several steps, including a review of the existing literature on the subject, an analysis of the complaints received and of inspection results, as well as interviews with banking and insurance professionals and the launch of a research project with researchers in economics of ageing in order to study more scientifically the behavior of this population towards financial products.

Example: the Central Bank of Ireland's Code of Conduct on Mortgage Arrears (CCMA) is intended to ensure fair and transparent treatment of financially-distressed borrowers and to ensure that each mortgage arrears case is considered on its own merits. Regulated entities must use the CCMA framework when dealing with borrowers in mortgage arrears or pre-arrears. In 2015, the Central Bank began a themed inspection of lenders' compliance with the CCMA. Overall, it was found that lenders have implemented frameworks as required by the CCMA; however, weaknesses, of varying degrees, were found, in some lenders' policies, procedures, systems and controls. Where poor practices were identified, the Central Bank instructed lenders to cease these practices immediately. Formal risk mitigation programmes were issued to a number of lenders and in the case of two lenders, identified as outliers, independent third party reviews were also required.

Example: since 2010, the Central Bank of Ireland has been identifying and pursuing some lenders in relation to so-called tracker related issues. These include borrowers who switched from their tracker rate and/or lost their right to revert to a tracker rate when they came to the end of a fixed-rate period on their mortgage. In December 2015, the Central Bank wrote to all lenders formally setting out the framework for an industry-wide review of tracker mortgage accounts (aka – the Tracker Mortgage Examination). Under this Examination, all lenders were required to examine the extent to which they were meeting their contractual obligations to customers. The Examination covers all lenders who may have sold tracker mortgages in the past, including those no longer selling mortgages and covers mortgages that have been redeemed or switched to another lender. Lenders were required to carry out a full review of the impacted customer's mortgage account. As at end-March 2018, approximately 37,100 accounts have been identified by lenders where a right to, or the option of, a tracker rate of interest and/or the correct tracker rate of interest was not provided to customers in accordance with lenders' contractual or regulatory requirements. €459m has been paid by lenders in redress and compensation to date with more to follow. While the Central Bank of Ireland believes that the majority of affected customers have been identified, there may be some further increase in the number of affected customers before the Tracker Examination is concluded in full.

Example: in March 2017, the Japan FSA published "Principles for Customer-Oriented Business Conduct" that comprises seven principles, including the need to clarify fees and provide easily understandable important information on sales of products. The JFSA encourages financial institutions to adhere to the Principles, and 1,679 financial institutions adopted them as at the end of June

2019. The JFSA continues to monitor the implementation. In addition, the JFSA also encouraged financial institutions to publish the common key performance indicators (KPIs) comparable across investment trust distributors to make their approaches more visible to customers, and 281 financial institutions published them as at the end of June 2019.

Example: the UK FCA has published a Call For Input on Access to Travel Insurance, which looked at the challenges for firms and consumers in providing and accessing fairly-priced cover for people with pre-existing medical conditions. The UK FCA wants to understand the market and consumers' journeys better and use this as an opportunity for industry, regulators and consumer groups to work together to produce meaningful change for vulnerable consumers.

Example: Portugal has in place a basic bank account regime since 2000. Under this legal framework, which was designed to promote financial inclusion, all deposit-taking institutions are obliged to provide low-cost essential banking services to citizens, including opening/maintaining a current account – the basic bank account – and instruments used for transactions on the account, such as a debit card. The Central Bank of Portugal discloses information on the basic bank account on its Bank Customer website and it conducts financial education initiatives on this issue. In order to allow consumers with disabilities to access to the information disclosed at the bank customer website, some of the contents have been made available on sign language.

17. Firms should ensure that computer programmes or algorithms underpinning digital financial services, such as digital financial advice, are designed to produce outcomes which are objective, consistent and fair for financial consumers, and which take account of their financial capabilities, situation and needs of their customers, including their level of digital literacy. The methodology and assumptions underpinning such programmes should be transparent, understood by the firm and capable of being explained.

Example: Germany: BaFin has analysed and highlighted issues relating to the use of algorithms in its report on Big Data and Artificial Intelligence (BDAI) published in June 2018. In particular, the report discusses scientific approaches that allow to make even very complex AI-models explainable. The report also states that the risk of consumer discrimination due to new technologies might increase and reach a new level as algorithms may focus on characteristics or attributes where differentiation is prohibited by law. In this regard, it stresses the importance of a "compliance-by-design"-approach when developing software solutions in this field.

Example: in March 2018, the ACPR in France launched a Task Force to tackle the opportunities and challenges raised by AI in the financial sector. This Task Force (TF) is composed of banks, insurance companies and fintechs. It also includes other authorities such as Data Protection Authority and Financial Markets Authority. The primary goal of this TF consisted of issuing a Discussion Paper in December 2018, which summarizes the implications of using AI and algorithm technologies in the financial sector.

18. Firms should approach algorithms and the potential risks arising in the same way they approach risks arising from other financial models. This includes ensuring proper documentation, oversight and testing the underlying assumptions with clear processes and expert and independent validation of the outcomes they produce.

> Example: in Germany, BaFin has highlighted these issues in its report on Big Data and Artificial Intelligence (BDAI) published in June 2018. One of the conclusions of the report is that when designing (wholly or partially) automated processes, it is important to ensure that they are embedded in an effective, appropriate and proper business organisation. Ultimately, responsibility for automated processes is to remain with the senior management of the supervised firm. Appropriate documentation is required to ensure this.

Principle 4: Disclosure & Transparency

Financial services providers and authorised agents should provide consumers with key information that informs the consumer of the fundamental benefits, risks and terms of the product. They should also provide information on conflicts of interest associated with the authorised agent through which the product is sold.

In particular, information should be provided on material aspects of the financial product. Appropriate information should be provided at all stages of the relationship with the customer. All financial promotional material should be accurate, honest, understandable and not misleading. Standardised pre-contractual disclosure practices (e.g. forms) should be adopted where applicable and possible to allow comparisons between products and services of the same nature. Specific disclosure mechanisms, including possible warnings, should be developed to provide information commensurate with complex and risky products and services. Where possible consumer research should be conducted to help determine and improve the effectiveness of disclosure requirements.

The provision of advice should be as objective as possible and should in general be based on the consumer's profile considering the complexity of the product, the risks associated with it as well as the customer's financial objectives, knowledge, capabilities and experience.

Consumers should be made aware of the importance of providing financial services providers with relevant, accurate and available information.

19. Ensuring that disclosure and transparency requirements are applicable and adequate to the provision of information through all channels relevant to digital financial services and covering all relevant stages of the product lifecycle. For example, policy makers should ensure that proportionate requirements are developed relating to the clear, simple and comparable disclosure of terms, fees and commissions.

> Example: in Italy, the Bank of Italy's regulation on the transparency of contractual conditions applies to the provision of financial services even when they are offered through digital channels. Furthermore, the regulation requires that information is easily accessible on the web site of the financial service providers and made available, via download, in the form of an information sheet.
>
> Example: in 2017, the Financial Consumer Agency of Canada (FCAC) conducted Public Opinion Research into clear language disclosure in paper-based financial statements.

20. Supporting consumer communications that are clear and simple to understand regardless of the channel of communication.

21. Evaluating existing disclosure requirements if required in the context of digital financial services, and if necessary, developing new requirements taking account of disclosure via digital means (e.g. minimum scroll down time for reading pre-contractual information).

> Example: in March 2017, the Japan FSA published "Principles for Customer-Oriented Business Conduct" that comprises seven principles, including the need to clarify fees and provide easily understandable important information on sales of products. The JFSA encourages financial institutions to adhere to

the Principles, and 1,679 financial institutions adopted them as at the end of June 2019. The JFSA continues to monitor the implementation. In addition, the JFSA also encouraged financial institutions to publish the common key performance indicators (KPIs) comparable across investment trust distributors to make their approaches more visible to customers, and 281 financial institutions published them as at the end of June 2019.

22. Embedding an understanding of consumer decision-making and the impact of behavioural biases in the development of policies relating to disclosure requirements and/or alternative approaches to ensure a customer-centric approach.

Example: in 2018, the European Commission launched a behavioural consumer study on the digitalisation of the marketing and distance selling of financial services. The purpose of this study is 1) to map the current landscape of providers using digital channels to market and sell retail financial services (types of providers, products and practices, notably in relation to information disclosure) in the EU28, Norway and Iceland; 2) to assess the impact of the commercial practices mapped on consumers' behaviours; and 3) to provide evidence to assess whether legislative updates or other follow-up actions are necessary.

23. Encouraging financial services providers to test digital disclosure approaches to ensure their effectiveness, taking into account factors such as different screen sizes, different communication formats etc. and recognising that there may be consumers in the target audience for the product or service who are not digitally literate.

24. Testing and exploring new ways of making disclosure more effective for consumers in terms of more targeted, proportionate and customer-centric approaches.

Example: the United Kingdom Financial Conduct Authority has a 'Smarter Consumer Communications' initiative to encourage ways to improve communication by firms to consumers – whether it is product features, terms and conditions, or other key communications. The aim is to look at opportunities to achieve more targeted, proportionate and customer-centric approach to disclosure. The project includes consideration of whether some regulatory requirements related to communications could benefit from a rethinking on their fitness-for-purpose in a digital age.

25. Monitoring financial services providers' disclosure practices in their provision of services provided through digital means, as well as disclosure practices of third parties involved in the offering of digital financial services. Examples of actions to be taken include:

- Reviewing financial institutions' disclosure practices in relation to products and services provided through digital channels, including what is disclosed, how it is disclosed, the timing and timeframe used for disclosure, how can customers confirm they have had access to the information, how can customers return to disclosure material provided in a digital format, how consumers can request additional information or clarification if need be etc. Such reviews could be conducted via mystery shopping exercises.[7]

[7] See for example: Mystery Shopping for Digital Financial Services: A Toolkit, Working Paper, CGAP and ITU, April 2017.

Example: the Central Bank of Brazil is still discussing the P2P lending specific regulation, but since 2015 some firms have started working P2P style transactions using some provisions of current regulatory framework, specifically the agent banking regulation. In that context, each firm was contracted as a banking agent by a financial institution. The Conduct Supervision department of the Central Bank took action to ensure that the activities were fully compliant with regulation, especially in terms of transparency and suitability.

According to current regulation in Brazil, the banking agent acts for and under the guidelines of the contracting institution, the latter assuming full responsibility for the services rendered to clients and users and guaranteeing the integrity, reliability, safety and secrecy of the transactions carried out, as well as following the legislation and regulation applicable to these transactions.

The regulation requires that the banking agent to disclose its condition as a purveyor of services to the contracting institution, identified by the brand in the market, along with a description of products and services provided and telephone numbers of attendance services and customer relationship management unit of the contracting institution. In addition, the banking agents must use exclusively operational procedures and tables defined by the contracting institution, including the proposition or application of fees, interest rates, exchange rates and any other amount earned or owed by the client, inherent to the products and services supplied by the contracting institution. The institutions must also assure provision of information necessary for free choice and decision making by clients and users, explicitly referring to rights, obligations, responsibilities, costs and charges, penalties, and eventual risks involved in the execution of operations and rendering of services.

- Having access to information disclosed to clients contracting products or services through websites, apps and restricted websites (e.g. online banking)

  Example: the Bank of Portugal has required financial institutions information on the provision of consumer credit products through digital channels. The information requested includes a description of the features of the product and the contracting process, including the implemented security mechanisms, and the pre-contractual documents. With this initiative, Bank of Portugal aims to improve the supervision of the contracting process for consumer credit products via digital channels, namely on what concerns the compliance with disclosure requirement and to monitor the financial institutions practices when contracting through digital channels (https://clientebancario.bportugal.pt/pt-pt/noticias/banco-de-portugal-exigeinstituicoes-informacao-sobre-os-creditos-que-vao-comercializar). This also constitutes a way of testing a new oversight tool before new regulatory requirements are issued.

26. Ensuring that the provision of advice, including digital advice, is objective and based on the customer's profile, objectives, financial literacy and experience as appropriate. For example:

- Algorithms underlying the generation of digital advice are objective and consistent.
- Financial services providers ensure that the methodology underpinning digital advice services is clear and transparent, including options for recourse and that they lead to fair consumer outcomes.

27. Considering whether technological developments and the increasing availability of and access to data creates opportunities to test and develop alternatives to traditional forms of disclosure, for example, the publication of particular indicators relating to a financial product or service (e.g. consumer complaints) to assist in decision-making, "cooling on" periods to give consumers additional time to confirm their purchasing decision, "smart defaults" ensuring consumers are automatically defaulted to the best option for them; and "personalised friction" which allows consumers to create steps (such as tailored log-ins) to act as breaks in spending.

28. In relation to the disclosure of policies relating to the collection, storage or use of personal data which are reliant on the giving of consent by a consumer, considering ways of ensuring that requests for consent are as clear and understandable as possible. Consideration may be given to alternative or supplementary approaches, such as "privacy by design" (whereby data protection is embedded in the design of a product or system from the outset) or "data minimisation" (whereby only the minimum amount of data is collected and stored for the minimum amount of time). It is noted that not all public authorities responsible for financial consumer protection regulation have direct responsibility for data protection issues in their jurisdiction.

> Example: the issue of consent is addressed among other things by the General Data Protection Regulation (GDPR) developed by the European Commission and approved by the European Parliament and Council in 2016. The aim of the GDPR is to harmonise data privacy laws across Europe and protect consumers from privacy and data breaches. Under the GDPR, the conditions relating to consent have been strengthened, including that the request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent and that consent should be easy to withdraw. The GDPR also includes provisions relating to privacy by design.

> Example: work conducted for the World Economic Forum into the appropriate use of customer data includes a preliminary set of data principles, the first of which relates to consent. According to this preliminary principle, consent should be informed consent in that companies need to provide clear and accessible information about how customer data will be used.

Principle 6: Responsible Business Conduct of Financial Services Providers and Authorised Agents

Financial services providers and authorised agents should have as an objective to work in the best interest of their customers and be responsible for upholding financial consumer protection. Financial services providers should also be responsible and accountable for the actions of their authorised agents.

Financial services providers should assess the related financial capabilities, situation and needs of their customers before agreeing to provide them with a product, advice or service.

Staff (especially those who interact directly with customers) should be properly trained and qualified.

Where the potential for conflicts arise, financial services providers and authorised agents should endeavour to avoid such conflicts. Where such conflicts cannot be avoided, financial services providers and authorised agents should ensure proper disclosure, have in place internal mechanism to manage such conflicts, or decline to provide the product, advice or service.

The remuneration structure for staff of both financial services providers and authorised agents should be designed to encourage responsible business conduct, fair treatment of consumers and to avoid conflicts of interest. The remuneration structure should be disclosed to customers where appropriate, such as when potential conflicts of interest cannot be managed or avoided.

29. The objective to work in the best interest of the customer should be central to a firm's purpose irrespective of the channel(s) used to contract financial products or services.

> Example: in November 2016, the Central Bank of Brazil enacted Resolution nº 4.539 that requires financial institutions under its jurisdiction to set up an institutional policy on the relationship with financial consumers. This policy requires the institution's guidelines, objectives and core values to promote a sound corporate culture based on ethics, transparency, diligence and accountability, which are key elements for ensuring the convergence of interests and a corporate reputation perceived by the stakeholders as credible, reliable and competent. Financial institutions are expected to work with consumers in a cooperative and balanced manner, striving to treat them fairly and equitably throughout their relationship, including pre-contractual, contractual and post-contractual duties. This regulation was issued in order to support financial stability, as financial regulators should also prioritize safeguarding consumers' interests in order to improve public trust and confidence on the financial sector.

> Example: in Germany, one regulatory principle in financial markets supervision is that the management board of a supervised entity remains responsible for compliance with regulatory requirements, including in the event of outsourcing arrangements. Authorised retail agents, too, are regarded as employees of the supervised entity in respect of liability towards customers and supervisors. Conduct of business in the client's best interest being one of the very central regulatory requirements, the management board's responsibility ensures that supervised entities put sufficient focus on this topic.

Reduction of conflicts of interest can, among other measures, be achieved by providing financial services without taking commission from third parties. To increase transparency and provide information to the public Germany has established a publicly accessible online register of independent investment advising entities who follow such a strictly fee-based business approach.

Example: in March 2017, the Japan FSA published "Principles for Customer-Oriented Business Conduct" that comprises seven principles, including the need to clarify fees and provide easily understandable important information on sales of products. The JFSA encourages financial institutions to adhere to the Principles, and 1,679 financial institutions adopted them as at the end of June 2019. The JFSA continues to monitor the implementation. In addition, the JFSA also encouraged financial institutions to publish the common key performance indicators (KPIs) comparable across investment trust distributors to make their approaches more visible to customers, and 281 financial institutions published them as at the end of June 2019.

Example: in Italy, banks and financial institutions are required to set up internal procedures aimed at ensuring that transparency and fairness standards are complied with at any stage of the product distribution, including when distribution is carried out by third parties. In addition, banks and financial institutions are liable towards customers and supervisors for any misconduct of tied agents carrying out distribution of their products.

30. Financial services providers should provide customers with assistance as appropriate when selling a financial product or service through digital channels through, for example, explanatory notes attached to the pre-contractual information provided, FAQs specifically related to the product or service being sold, and/or providing the possibility of human interaction during the process (e.g. e-mail, telephone).

Example: the Central Bank of Portugal requires that during the pre-contractual phase information is made available to consumers through online and mobile channels. Within its oversight capacity, the Central Bank of Portugal assesses whether the information mechanisms provided are adequate. They should clearly convey information on the characteristics of the credit product and allowing clients to consider if the proposed product is appropriate to their needs and financial situation. The central bank also evaluates whether contracting processes on digital channels incorporate the required means to clarify the doubts and questions of the customers, in particular warnings and information notes, access to pages with answers to FAQs, free phone support, access to chat with an institution's assistant, or chatbot.

Example: in Hong Kong, specified types of life insurance products are exempted from the requirement of financial needs analysis if such products are distributed through digital channels without recommendation. For such products, insurers and banks are required to provide clearly and prominently certain important information and warnings regarding the product (e.g. product type and nature, target premium amount, payment period and benefit periods of the product and warnings concerning affordability and liquidity risk associated with the product) on the digital distribution channel. On product type and nature, insurers and banks are required to disclose on the digital distribution channel that the product is underwritten by an insurance company and is neither a bank deposit nor saving plan of a bank.

Example: in Hong Kong, the HKMA requires banks to take proactive steps to ensure that their lending business is conducted in a responsible manner and that borrowers understand the key features, terms and conditions of the credit products, and their repayment obligations. When designing their online finance platforms or applications, banks should consider the use of proper tools such as pop-ups and hyper-linked text to provide customers with adequate information and adequate chance to consider the implications of their borrowing behaviour in order to enable them to make informed borrowing decisions.

Example: the Bank of Italy provisions on financial consumer protection (i.e. provisions on "Transparency of contractual conditions. Fairness of the relationships between financial institutions and customers") require banks and other financial institutions granting credit to set up internal procedures aimed at ensuring that consumers are provided with adequate explanations on the credit contract in order to assess whether the proposed credit agreement is adapted to their needs and to their financial situation. The assistance includes, for example, explanations regarding the pre-contractual information, the main characteristics of the products proposed and the effects they may have on the consumer, including the consequences of default in payment by the consumer.

Example: according to the Spanish Ministerial Decree EHA/2899/2011, of 28 October, for banking services provided through distance communication means, the financial provider must facilitate to consumers a telephone number in a visible place, in order to solve any problem during the contracting process.

31. Consumers should receive explicit information on the true contractual party involved in the provision of the financial product or service through digital means, e.g. services provided by online aggregators or brokers. Where there are multiple entities involved, on the identification and responsibilities of each party involved in the transaction.

Example: FCAC provided guidance to payment card network operators (PCNOs) that operate in Canada and their participants including card issuers and acquirers, independent sales organizations (ISOs) and other service providers such as terminal leasing firms. The guidance provided examples of information summary boxes, for illustrative purposes, to clearly set out FCAC's expectations in relation to this requirement

32. Financial services providers should not pass on customer details, including payment details, to third parties without seeking the consumer's informed and explicit consent.

Example: under the EU General Data Protection Regulation, personal data must be processed in a lawful and transparent manner and the collection of personal data should be processed for specified, explicit and legitimate purposes and in a manner that is compatible with the initial purpose. As such, consumers should be informed about all the purposes of the processing for which their personal data are intended and all the recipients of their personal data, in order to provide an informed and explicit consent.

33. Firms should take into account the potential differences in consumer behaviour when transacting online versus more traditional methods of transacting, e.g. more frequent access of digital financial services (e.g. mobile banking), different levels of financial capability, potentially shorter attention spans when transacting online etc.

Example: the Central Bank of Portugal, within its oversight capacity and based on the information reported, has been reflecting with institutions on the requirements applicable to consumer credit products and also considering behavioural economics' insights. As such, the central bank has been monitoring the way institutions ensure, on digital channels, information (e.g. compulsory scroll-down of the Standard European Consumer Credit Information Sheet) and assistance obligations (e.g. FAQ, chatbot and/or helpline on the credit product and borrowing process) and how clients may exercise the rights of withdrawal and early repayment. The Central Bank of Portugal also holds bilateral meetings with institutions for the demonstration and detailed analysis the available contracting flows on online or mobile channels.

34. Financial services providers are responsible for the services, advice or recommendations generated by computer programmes and algorithms underpinning digital advice services.

35. When using computer programmes for decision-making, such as automated credit scoring models, firms should make sure they are robust, appropriately weight all relevant variables, and where necessary or requested by the consumer provide the possibility of manual intervention, to mitigate against irresponsible lending decisions or decisions based only on the result of the credit score.

Example: the Italian regulation requires banks and other financial institutions granting credit to assess the consumer creditworthiness before the conclusion of the contract and in case the parties agree to change the total amount of credit after the conclusion of the contract.

Example: in Portugal, credit institutions are required to assess the customer's capacity to repay before selling a credit product or increasing the total amount of a loan already contracted. The Central Bank of Portugal requires that, for credit agreements that are in excess of an amount of ten times the legal minimum wage, credit institutions must carry out an individual assessment of the customer's capacity to reimburse the credit, taking into consideration the customer's level of regular income and expenses. If the credit agreement is for less than that amount, credit institutions are allowed to estimate the customer's income and expenses on the basis of credit-scoring models. This solution allows for faster credit-granting processes, which are essential in a growing digital consumer credit market, where convenience and speed are critical factors.

36. Firms should ensure that financial products, services and distribution channels are aligned with the relevant interests, characteristics and objectives of the "target market".

Example: in Italy, the Bank of Italy provisions on financial consumer protection, as recently amended in order to implement the EBA Guidelines on product oversight and governance, require banks and other financial institutions to have in place internal procedures aimed at ensuring that retail banking products are manufactured and distributed in accordance with the interests, objectives and characteristics of the group of customers for whom each product is designed (i.e. target market).

Example: the Central Bank of Ireland undertook research in 2017 to examine consumer experiences when purchasing gadget insurance. The research

examined the attitudes and behaviours of consumers and the influence of any biases, which may have impacted on their ability to make informed decisions and confident claims on their gadget insurance. The research found that most consumers did not plan to buy gadget insurance until it was sold to them as an add-on at the point of sale; most purchases were based on verbal explanations of retail staff selling the gadget and consumer trust in their provider; the majority of consumers did not understand their cover and thought it covered more than it did; and some consumers may have been paying for cover they do not need. Along with this research, the Central Bank undertook a thematic inspection[8] on the sale of gadget insurance products in relation to product oversight and governance requirements in 2018. Upon the conclusion of this themed inspection, formal feedback will be provided to the Irish insurance industry, as a whole. The findings from thematic inspections will also published on the Central Bank of Ireland's website.

Example: in Japan, according to the "Comprehensive Guidelines for Supervision", financial institutions are required to ensure that investment solicitation is conducted in an appropriate manner suited to their customer's attributes by offering transactions with terms and contents that are commensurate with the customer's knowledge, experience, asset status and investment purpose as well as his/her ability to make judgments regarding risk management. It also requires that careful attention should be paid to Internet transactions in particular in light of the absence of face-to-face contact.

Example: the European Banking Authority's Guidelines on product oversight and governance and, on the insurance side, the delegated regulation supplementing Directive (EU) 2016/97 of the European Parliament and of the Council with regard to product oversight and governance requirements for insurance undertakings and insurance distributors, define requirements for manufacturers and distributors when designing and distributing financial products and services. Those Guidelines, apart from setting that manufacturers should identify the relevant target market of a product, ensuring its suitability according to interests, objectives and characteristics of that market, also sets that the manufacturer should select distribution channels that are appropriate for that particular segment and monitor that the products and are distributed to consumers included in that target market.

Example: in Portugal, credit institutions are required to establish specific procedures for the governance and monitoring of deposits and credit products, ensuring that banking clients' interests, objectives and characteristics are considered when those products are created and commercialized. Credit institutions are also required to comply with rules concerning the assessment and suitability of structured deposits to the knowledge and experience of their banking clients (Law no. 35/2018).

37. Firms should ensure their recruitment processes are tailored to identify employees that will embrace the firm's culture and act in line with the firm's purpose.

[8] Thematic or themed inspections focus on a specific topic or product rather than on a specific institution. These inspections are carried out on a number of regulated entities for which the topic would be applicable or those that represent a significant portion of the market share of the relevant product.

38. Firms should ensure that their staff understand what is acceptable and unacceptable behaviour, and know what behaviours/decisions will be valued and rewarded (those in line with the firm's purpose). Firms should ensure that their internal policies and procedures/codes of conduct contain guidance, as appropriate, on responsible business conduct, best interests principles, sales processes etc.

> Example: in Hong Kong, the HKMA provided guidance in March 2017 for banks to develop and promote a sound corporate culture. In particular, with respect to governance, a dedicated board-level culture committee (or an appropriate board-level committee) should, among others, approve, review and assess, at least annually, the adequacy of any relevant statement which sets out the institution's culture and behavioural standards, and seek to ensure that such statement is translated into policies and procedures (including training) that are relevant to the day-to-day work of different levels of staff.
>
> Example: in Italy, the Bank of Italy provisions on financial consumer protection, as recently amended in order to implement the EBA Guidelines on remuneration policies and practices related to the sale and provision of retail banking products and services, require banks and other financial institutions to adopt remuneration policies that do not introduce incentives for their sales staff to favour their own interests, or the institution's interests, to the detriment of customers. . .
>
> Example: the UK FCA introduced its Senior Managers and Certification Regime (SM&CR) to reduce harm to consumers and strengthen market integrity by making individuals more accountable for their conduct and competence. The SM&CR aims to:

- encourage a culture of staff at all levels taking personal responsibility for their actions; and
- make sure firms and staff clearly understand and can demonstrate where responsibility lies

> Example: in Portugal, there are rules defining general conduct duties. It is foreseen that administrators and employees of credit institutions must act with due diligence, neutrality, loyalty and discretion, and respect for the interests entrusted to them, both in relations with clients and in relations with other institutions. It is also foreseen general technical competence requirements. In the last years, it has been implemented new conduct duties in order to promote the prevention of conflicts of interest and a customer centric approach, in particular concerning sales incentives and the training of staff in certain issues. The Central Bank of Portugal is responsible for certifying entities that provide training to institutions' employees who sell mortgage credit and to credit intermediaries. Employees are required to have high levels of competences and skills, in order to carry out their tasks with quality and efficiency and to be able to provide complete information to clients (Decree-Law no. 74-A/2017). Also, credit intermediaries must have an adequate level of knowledge and expertise in the issues relevant for their activity (Decree-Law no. 81-C/2017). These applies whether those entities operate through traditional or digital channels.
>
> Regarding the employees involved in the commercialisation of structured deposits (under the supervisory scope of the Central Bank of Portugal), credit

institutions are also required to ensure that they have the adequate knowledge and skills (Law no. 35/2018).

39. People-related policies and practices should be designed to promote and embed appropriate behaviours and deliver appropriate outcomes in addition to remuneration structures.

Example: in Hong Kong, the HKMA provided guidance in March 2017 for banks to develop and promote a sound corporate culture. In particular, with respect to incentive systems, the incentive systems of an authorized institution (including staff recruitment, performance management, remuneration and promotion systems) should not only reward good business performance but also take into account adherence (and non-adherence) to the institution's culture and behavioural standards, with a view to avoiding incentivising short-term business performance at the expense of the interests of customers and the safety and soundness of the institution. There should be clear and appropriate consequences established, articulated and applied for individuals engaging in any undesired or unacceptable behaviours. Furthermore, for an incentive system to be effective, the relevant arrangements and/or remuneration structure for different levels of staff and management should be commensurate with their respective seniority and responsibilities.

Example: in 2017, the Central Bank of Ireland undertook research in order to gather evidence on consumers' awareness and understanding of how financial advisers were paid and how commissions work; consumers' attitude towards for an upfront fee or a commission structure; consumers' understanding of and preference for dealing with independent advisers and consumers' attitudes/opinions towards financial advisers e.g. levels of trust, having customers' best interests in mind. The research involved 506 consumers. Of these, 29% of respondents did not know how an independent adviser was paid and although 55% of respondents said they understood that financial advisers were remunerated by means of a commission payment, the majority of respondents, (across all product areas), said they were not aware of any ongoing commission payments from the product producer to the financial adviser. On foot of this research, the Central Bank of Ireland published a Consultation Paper (January 2018) in which it explored the pros and cons of introducing a ban or restriction on the payment of commissions to intermediaries.

Example: in Portugal, credit institutions whose workers are involved in the selling of deposits and credit products are required to comply with rules on remuneration and performance assessment, avoiding conflicts of interests that might undermine the protection of banking clients (Law no. 35/2018). The Central Bank of Portugal also issued rules on mortgage credit regarding the definition, approval and monitoring of remuneration policies ensuring they do not favour the interests of the institution or its employees to the detriment of consumers. Remuneration policies must, for example, ensure a balance between the fixed and variable components of remuneration, making the latter depending also on qualitative criteria, such as the quality of services provided (Notice no. 5/2017).

Example: Banco de España Circular 5/2012, of 27 June, establishes that commercialization of products policies should include remuneration criteria that promote the compliance of responsible business conduct principles.

Principle 7: Protection of Consumer Assets against Fraud and Misuse

Relevant information, control and protection mechanisms should appropriately and with a high degree of certainty protect consumers' deposits, savings, and other similar financial assets, including against fraud, misappropriation or other misuses.

Related OECD instruments

The following OECD instruments are relevant:

- OECD Recommendation on Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders (2003)
- OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007)
- OECD Consumer Policy Guidance on Mobile and Online Payments (2014)
- OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (2015)
- OECD Recommendation on Consumer Protection in E-Commerce (2016)
- OECD Recommendation on Artificial Intelligence (2019)

40. Policy makers and oversight authorities should ensure they have the necessary technological capacity, resources and supervisory tools to oversee the measures implemented by financial services providers to mitigate digital security risks and react to digital security incidents where the financial assets of consumers are at risk.

> Example: the French Banking and Insurance Supervisory Authority (ACPR), in cooperation with a department of the French Central Bank dedicated to payment security, pays particular attention to digital security risks and IT resources when authorising credit institutions, payment institutions, e-money institutions and insurance firms. On a permanent basis, the ACPR also oversees these risks and resources as part of its on-site and off-site inspections as well as through its internet watch.
>
> Example: the German Federal Financial Supervisory Authority (BaFin) pooled key skills throughout its organisation to establish the IT Supervision Payment Transactions and Cyber Security Directorate (GIT) in 2018 in order to engage in effective prevention measures in cooperation with financial firms. This cross-sectoral Directorate focuses on, among other matters, policy issues relating to cyber security, operational supervision of payment institutions and e-money institutions, policy issues relating to IT supervision and the inspection regime as well as IT inspections at banks, insurance undertakings and German asset management companies.
>
> Example: the Hong Kong Monetary Authority ("HKMA") has established a specialised subject team focusing on technology risk under the Banking Supervision Department since early 2000s. Considering the growing use of fintech and a challenging cyber threat landscape in recent years, the HKMA has further stepped up its supervisory capacity on technology risk.

Example: in Italy, the Bank of Italy oversees – also through onsite inspections – the way financial services providers handle risks related to the activities they perform, including security risks.

Example: Banco de Portugal has a Cybersecurity Center whose objective is to promote cybersecurity as well as to minimize cyber risk associated with Banco de Portugal's activity. Externally, the Cybersecurity Center is the official CSIRT (Computer Security Incident Response Team) of Banco de Portugal, having as main activities: (i) institutional collaboration with counterpart entities at Eurosystem level and participation in working groups and reflection on related issues; (ii) to ensure the functioning as Sectoral CSIRT, associated with the banking and financial system, implementing and managing the portfolio of associated services; (iii) the provision of strategic and technical advisory services to external entities, namely in support of the coordinated response to a cyber-incident; (iv) to promote partnerships and development of cooperation and collaboration channels with third parties; and (v) to ensure executive and trend reporting, as well as benchmarking with other institutions, specifically at the national and Eurosystem sectoral level.

In 2019, Banco de Portugal created an Innovation Lab which aims to catalyse an innovative mind-set within the institution and to support its decision making. The main motivations for launching inov# comprise: (i) technological and process evolution (how a supervisor may, on the one hand, take proper advantage of these technological paradigms – such as artificial intelligence, machine learning and blockchain – to fulfil its mission and, on the other hand, obtain relevant knowledge to assess risks and potential constraints such developments may entail for the financial system); (ii) internal and external demand (internally, Banco de Portugal is assessing the feasibility of using these new technologies to streamline current supervisory processes and to identify new working methods; externally, many financial service players seek clarification from Banco de Portugal on innovative products and services); (iii) European System of Central Banks (ESCB) collaboration.

41. Policy makers and oversight authorities should work collaboratively with industry, other regulatory and supervisory authorities and law enforcement agencies (including agencies responsible for digital security policy making, implementation, information sharing and trend monitoring), to share information and understand emerging trends relating to new types of digital financial frauds and scams. Information sharing and monitoring arrangements that may support this collaboration include the Financial Services Information Sharing and Analysis (FS-ISAC) and various types of CERTs (computer emergency response teams).

Example: In France, the ACPR is working with the French Market Authority (AMF) within a joint unit created in 2010 for financial consumer protection purposes. Main missions of this unit are to share information and knowledge on emerging trends and new types of digital financial frauds and scams, and to coordinate inspections accordingly. The ACPR is also closely working with the French Directorate-General for Competition, Consumer Affairs and Prevention of Fraud (DGCCRF) in particular on internet watch and digital scams. In addition, the ACPR holds on a quarterly basis a consultative commission on business practices and consumer protection issues composed of representatives from banking and insurance industry and civil society.

Example: in Hong Kong, China the HKMA works with the banking industry, the Hong Kong Police Force ("HKPF") and other local regulators to share information and understand the emerging digital financial frauds and scams. Observations related to emerging fraud cases would be shared with the banking industry, the HKPF and other local regulators during regular meetings or ad-hoc sharing sessions. The information of the fraud cases was also shared with certain overseas regulators under bilateral information sharing arrangements.

Example: Italy has established the Italian Payments Committee (IPC), which is a cooperation forum whose main objective is to foster the development of a secure, innovative and competitive market for private and public payments in Italy able to respond to global challenges and to meet the needs of users. This Committee provides a permanent forum for discussing key issues pertaining to the payment industry and plays a role of point of contact vis-à-vis other national and European committees/fora. The IPC is chaired by the Bank of Italy; its members are representatives of the supply and demand side of the market (representatives of the banking community, payment institutions, retailers and consumers), payment service providers (banks, post office, payment institutions), technical service providers and the Public Administration. The IPC usually gathers in plenary sessions but ad hoc working groups may be set up in order to perform technical activities or address urgent matters; among these matters, also issues related to security of payments are discussed.

Example: in Portugal, under the regulatory framework applicable to the provision of payment services, financial services providers shall notify Banco de Portugal, without undue delay, in the case of a major operational or security incident.

Example: In Greece, the new Consumer Agenda promotes the ongoing evaluation of the Directive on Consumer Credit (2008/48), focusing on whether original objectives and tools of the Directive correspond to current needs, and the review of the Directive on the distance marketing of consumer financial services (2002/65), which will ensure better understanding of retail financial products taking into account the digitalisation in the provision of such products. It will aim at providing better protection for consumers from irresponsible lending practices, particularly those spread online.

42. Policy makers and oversight authorities should work collaboratively with foreign counterparts and relevant international organisations and networks to share information and intelligence about such frauds and scams that have cross-border aspects.

Example: The HKMA has established bilateral cybersecurity information sharing ("BCIS") arrangements with other overseas regulators since 2018 with an aim to share cybersecurity information in order to better protect financial systems against cyber-attacks. Through these BCIS arrangements, the HKMA has shared intelligence on frauds and scams with other financial regulators. To further strengthen the information and intelligence sharing among different jurisdictions, the HKMA has subscribed a multi-lateral information exchange platform which is designed for central banks and entities with supervisory or regulatory responsibility for financial institutions to distribute rapidly information on cyber threats, vulnerabilities, incidents and other threat intelligence that can impact financial services. In addition, the HKMA has obtained threat intelligence regularly from a global payment service provider's information sharing and analysis centre so as to

keep pace with the cyber threats trends, especially those frauds may have a wide-spread impact across borders.

Example: Under the regulatory framework applicable to the provision of payment services, Banco de Portugal, without undue delay, should provide the relevant details of a security incident to the EBA and the ECB. These entities, in cooperation with Banco de Portugal, assess the relevance of the incident to other relevant national authorities and shall notify them accordingly.

43. Oversight authorities should conduct ongoing monitoring, including collecting data and information from industry, to ensure awareness of developments in the market and the main digital security risks, for instance, innovative payments' solutions and precautionary measures to mitigate digital security risks. This could include mandatory reporting by financial services firms where necessary and appropriate. The OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity provides guidance for strategic approaches to the management of digital security risk aimed to optimise the economic and social benefits expected from digital openness.

Example: in France, pursuant to the provisions of Article L.521.10 of the Monetary and Financial Code, payment service providers – credit institutions, payment institutions and electronic money institutions – have to notify the ACPR and the Banque de France if any major operational and security incidents related to their payment services occurs. This reporting has to be made according to the methodology defined in the guidelines of the European Banking Authority (EBA/GL/2017/10).

Example: in Italy, payment services providers are required to report to Bank of Italy any major incident related to payment services.

Example: In 2016 and 2018, Banco de Portugal launched a 'Questionnaire on banking products and services through digital channels'. The questionnaire was sent to the main financial institutions operating in Portugal. The Questionnaire's goals were to assess the development of digital financial services in Portugal, the levels of adoption and use by customers, the constraints and obstacles to the demand for digital channels, and the main risks associated with the provision of financial services through digital channels and the mechanisms put in place to mitigate them.[9]

44. Policy makers and oversight authorities should work with industry, digital security and law enforcement agencies to explore role of technological innovation to detect and combat fraudulent behaviour targeting financial consumers, for example through the use of artificial intelligence to identify and block phone numbers used for voice phishing or identify potential harmful emails.

Example: in France, the ACPR set up a FinTech Innovation Unit in June 2016 to provide guidance to innovative players as regards their regulatory responsibilities and to interact with established players on their digitalisation transformation.

[9] https://clientebancario.bportugal.pt/en/noticias/press-release-banco-de-portugal-commercialisation-banking-products-and-services-digital; https://clientebancario.bportugal.pt/en/publicacao/commercialisation-banking-products-and-services-digital-channels-portugal-2018 .

Example: The HKMA has launched a series of Regtech-related initiatives since 2018 to facilitate the adoption of Regtech in Hong Kong. In particular, the HKMA has opened up the Fintech Supervisory Sandbox to Regtech projects or ideas raised by banks or tech firms. The HKMA has also been reaching out to the banking industry and tech firms to understand the latest Regtech use cases for prudential risk management. In particular, a growing number of use cases of Regtech in the areas of cybersecurity, fraud monitoring, credit risk management and regulatory compliance were observed.

45. Policy makers and oversight authorities should work with financial service providers to ensure that the application of arrangements for limitations on liability of financial consumers for fraudulent or unauthorised transactions extend to new types of mobile or online transactions (for example "push payments").

Example: in France, according to national provisions implementing the European Payment Services Directive (PSD2), rules on limited consumer liability for fraudulent or unauthorised transactions apply to all kinds of payments, including mobile and online transactions.

Example: In Hong Kong, according to the "Code of Banking Practice" which is issued jointly by the Hong Kong Association of Banks and the DTC Association in Hong Kong, and endorsed by the HKMA, a customer should not be liable for any direct losses suffered by him/her as a result of unauthorized transactions conducted through his/her account unless he/she acts fraudulently or with gross negligence. This principle is applicable to any banking products/services including digital ones. In addition, the HKMA issued a circular in October 2019 regarding consumer protection measures in respect of Open Application Programme Interface ("API"). The circular requires banks to, among others, (i) establish clear liability and settlement arrangement with their partnering third-party service providers ("TSPs") for compensating customers' loss arising from unauthorized transactions, with clear communication to customers upfront; and (ii) adhere to the principle that a bank customer should not be responsible for any direct loss suffered by him/her as a result of unauthorized transactions conducted through his/her account attributable to the services offered by the TSPs using Open API unless the customer acts fraudulently or with gross negligence.

Example: in Italy, according to national provisions implementing PSD2, rules on limited consumer liability for fraudulent or unauthorised transactions apply to all kinds of payments, including mobile and on line transactions.

46. Policy makers and oversight authorities should work collaboratively with relevant stakeholders, including other government and regulatory agencies, digital security agencies, law enforcement agencies, financial services industry and utility companies, to run and/or participate in campaigns to raise public awareness of digital security risks and promoting safe online and digital transactions.

Example: in France, a website (www.abe-infoservice.fr) held jointly by the ACPR, the Banque de France and the AMF provides practical information on banking, insurance and financial investment products as well as pedagogical videos to help the public against frauds and scams. In particular, black lists of unauthorised entities are regularly updated on this website. Key tips when choosing online or mobile banking services, published by the European Banking Authority and most national authorities from European Union, are also available on this website to help

consumers to protect themselves against fraud and other risks. On 17 September 2019, the ACPR, the AMF and the Paris public prosecutor held a press conference on frauds and scams, to encourage the public to become informed on fraudsters' operating procedures.

Example: In Hong Kong, the HKMA conducts consumer education programme to promote "smart and responsible" use of banking and financial services, including internet banking, mobile banking, and other digital financial services such as using bank smartphone apps or e-wallets in conducting peer-to-peer fund transfers. To reach the public, relevant messages (including cybersecurity tips and reminders to stay vigilant against cyber scams) are disseminated via TV commercials, radio clips, social media videos, educational leaflets, roving exhibitions and other promotion on HKMA's social media platforms including official Facebook page, LinkedIn, Instagram, and YouTube, HKMA's Information Centre and Coin Carts, as well as print media, cinemas, out-of-home and other digital platforms.

Apart from the aforesaid publicity campaigns, the HKMA has been partnering with other organisations to launch publicity campaigns to raise public awareness on information security. For example, the HKMA co-organised a campaign with the Hong Kong Police Force, Office of the Government Chief Information Officer and Hong Kong Computer Emergency Response Team to raise public awareness of cybersecurity and enhance public's vigilance to cyber scams.

Example: In Portugal, the three financial supervisors (the Central Bank of Portugal, the Portuguese Securities Market Commission and the Insurance and Pension Funds Supervisory Authority) established a partnership with a broad set of entities (including government ministries, financial sector associations, consumer associations, corporate associations and trade unions) to develop financial education initiatives under the National Plan for Financial Education. This National Plan included digital financial literacy as one of the priorities for the period 2016-2020, "to deepen knowledge and skills in using digital financial services". Several financial literacy initiatives were conducted focusing on digital security and fraud prevention, targeting different groups of the population.

Banco de Portugal runs awareness campaigns focused on the digital ecosystem on its Central Bank Customer Website (https://clientebancario.bportugal.pt/en/). "Protect yourself from online fraud" is an awareness campaign on prevention of on-line fraud that includes a brief description of fraudulent methods like phishing, pharming and spyware, and a set of security precautions that payment service users should follow to prevent security risks (https://clientebancario.bportugal.pt/pt-pt/noticias/proteja-se-contra-fraude-na-internet-banco-de-portugal-divulga-boas-praticas-nas-operacoes - only available in Portuguese).

Banco the Portugal launched the campaign "5 tips for staying safer online" ("#toptip" digital financial education campaign on security procedures to be adopted by youth) raising awareness among school-age children of precautions to take when using digital channels to access banking products and services (https://clientebancario.bportugal.pt/en/material/5-tips-staying-safer-online-toptip). The five suggested tips to stay safe online, to prevent fraud and over-indebtedness are: (i) "Don't make the internet a high-risk gamble"; (ii) "Your phone says a lot about you"; (iii) "Think before you post"; (iv) "Don't be tricked"; (v) "Don't give in to fraud". A printed brochure with the 5 #toptips and recommendations was distributed to all secondary schools and school libraries

across the country. Face-to-face training sessions take place in national schools, complementing the use of digital channels such as the Central Bank Customer Website.

The Central Bank Customer Website also identifies the major security risks raised by digital payments, as well as a set of security precautions to mitigate online fraud. The information provided is updated in keeping with the rapid development of financial innovation (e.g. "Digital security - why it is important" https://clientebancario.bportugal.pt/en/digital-security-why-it-important).

47. Policy makers and oversight authorities should participate in or consider the establishment of networks or communities of practice among agencies and industry to promote sharing of experiences of digital security risks including threats, vulnerabilities, incidents and mitigation measures. Information sharing and monitoring arrangements that may support this include the Financial Services Information Sharing and Analysis (FS-ISAC) and various types of CERTs (computer emergency response teams).

Example: in June 2019, the ACPR participated, among 24 other authorities, to the first cyber-crisis simulation exercise affecting the G7 financial system. The objective was to test the exchange protocol between the financial authorities via the simulation of a significant disruption of the financial system caused by a major cyber incident. This exercise coordinated by the Banque de France and carried out over three days, involved 24 financial authorities from 7 countries.

Example: The HKMA has regular dialogues with law enforcement agencies and regulatory bodies in Hong Kong. Formal bilateral liaison meetings or informal meetings are held with the Hong Kong Police Force and other local regulators, in which information on the latest trends and modus operandi of banking-related frauds, cyberattacks and incidents as well as relevant preventive and responsive measures is exchanged. The HKMA also meets with the Hong Kong Association of Banks and shares the latest trend on cyberattacks and good practices of cyber security controls regularly. In addition, as one of the pillars of the Cybersecurity Fortification Initiative implemented by the HKMA in 2016, a Cyber Intelligence Sharing Platform is available to provide an effective infrastructure for sharing intelligence on cyberattacks, and facilitating the timeliness of receiving alerts or warnings in relation to cyber threats.

48. Policy makers and oversight authorities should participate in or consider the establishment of dedicated reporting channels for financial consumers to report frauds and scams and, where they exist, ensure that they are up to date in terms of categorisation of online and mobile frauds and scams to support data collection and law enforcement, including in relation to cross-border activity where relevant. Where relevant, this should be done in coordination with digital security and law enforcement agencies.

For example: in France, financial consumers may report frauds or scams by phone or through the website ABEIS (mentioned above). They may also contact the French Directorate-General for Competition, Consumer Affairs and Prevention of Fraud (DGCCRF), working in close relationship with the ACPR.

49. Oversight authorities should use complaints handling data and analysis to identify potential security breaches/incidents, risks as well as the best practices adopted by financial services providers.

Example: in France, the ACPR collects on a yearly basis information about business practices and complaints handling from banks, payment institutions and e-money institutions. Any information relating to security breaches/incidents arising from this reporting is taken into account for supervisory activities.

Example: In Hong Kong, the HKMA handles customer complaints about banking products and services. The information received by the HKMA in handling complaints may assist it in identifying issues of supervisory or disciplinary concern that require follow-up actions. In addition, the HKMA would highlight the latest complaint trends, emerging topical issues, and share good practices through issuing Complaints Watch, a periodic newsletter, to promote proper standards of conduct and prudent business practices among banks. Topics such as recommendations on effective complaint handling and protection of customers' personal data have been shared with the banking industry in this connection.

Example: in Italy, Bank of Italy regularly collects on a yearly basis information about complaints addressed to banks and other supervised institutions (including payment services providers); where risks related to security breaches/incidents are detected through the analysis of complaints' data, this information is taken into account for supervisory activities.

Example: in Portugal, Banco de Portugal uses the information provided by complaints handling to set on-site inspections, to request the implementation of risk mitigation measures, to plan awareness campaigns and education initiatives, and to conduct closer monitoring of specific supervised institutions' security procedures.

50. Policy makers and oversight authorities should request that financial services providers report to oversight authorities statistical data on fraud activity, in particular concerning payment services, at least on an annual basis.

Example: in France, pursuant to the provisions of Article L. 521-10 of the Monetary and Financial Code, payment service providers - credit institutions, payment institutions and electronic money institutions - have to notify the ACPR and the Banque de France if any major operational and security incidents related to their payment services occurs. This reporting has to be made according to the methodology defined in the guidelines of the European Banking Authority (EBA / GL / 2017/10).

Example: In Hong Kong, the HKMA conducts Operational Risk Management Data Submission Exercise on an annual basis, in which the HKMA requests the participating banks to report, amongst others, the statistical data on the operational loss amount related to fraud events. Where appropriate, the analysis results on the data will be used to facilitate ongoing supervision and supervisory planning.

Example: in Italy financial services providers are required to submit to ECB or to Bank of Italy a yearly report on the analysis of security risks related to payment services.

51. Policy makers and oversight authorities should ensure that financial services providers are required to continuously assess the digital security risk to the services they provide, adopt appropriate security measures to reduce the risks, and inform financial

consumers of the security procedures that should be adopted to minimise the risk of online fraud. 10

> Example: The HKMA's Guideline on Supervision of Stored Value Facility Licensees sets out the high level supervisory principles that the HKMA adopts in assessing the fitness and propriety of SVF licensees, including requirements that licensees should set out and explain clearly the key features, risks, terms and conditions, and applicable fees, charges and commissions of its schemes, facilities, services and products. Additional disclosures, including appropriate warnings, should also be developed by the licensees to provide information commensurate with the nature, complexity and risks of the schemes, facilities, services and products.
>
> Example: in Italy, Bank of Italy provisions on financial consumer protection require payment services providers to disclose – among others – the security measures that customers are required to adopt when using payment instruments.
>
> Example: in Portugal, under the regulatory framework applicable to payment services, financial service providers shall disclose a set of information to consumers, including on the features of the services they offer, the security procedures to be adopted by consumers to minimise the risk of fraud and the redress mechanisms, before the conclusion of the contract.

52. Policy makers and oversight authorities should ensure that financial services providers have in place a digital security risk management framework, defining, for example, security objectives, roles and responsibilities. This framework should be documented, approved and periodically reviewed.11 The security risk framework should include appropriate evaluation of the cyber resilience of third party providers, where financial service providers outsource activities or the provision of digital services to such third party providers.

> Example: in Italy, financial services providers are required to have in place internal procedures for risk management, which shall take into account all operational and security risks related to payment services; such procedures shall also identify the mitigation measures adopted to protect customers against security risks, including frauds and illegal usage of personal data. The internal policy on security risks has to be approved by the management body and periodically reviewed.
>
> Example: in Hong Kong, as far as the banking sector is concerned, the HKMA has put in place a supervisory framework for supervising the cyber resilience of banks and bank's cyber security risk management. In September 2015, the HKMA issued a circular which highlighted the cyber security risk management practices that warrant banks' special attention. A credible benchmark of cyber security controls should be endorsed by the Board of a bank. Specifically, the HKMA has implemented Cybersecurity Fortification Initiative since 2016, which is underpinned by three pillars:

- Cyber Resilience Assessment Framework ("C-RAF"), which is a risk-based framework for institutions to assess their own risk profiles and benchmark the level

[10] See in particular: OECD Recommendation on Digital Security Risk Management for Economic and Social Prosperity (2015

[11] Ibid

of cyber defence and resilience that would be required to accord appropriate protection against cyber attacks. C-RAF comprises three stages of assessment: (i) Inherent Risk Assessment – It facilities an institution to assess its level of inherent cybersecurity risk and categorise it into "low", "medium" or "high" in accordance with the outcome of the assessment; (ii) Maturity Assessment – It assists an institution in determining whether the actual level of its cyber resilience is commensurate with that of its inherent risk. It covers seven key aspects, including governance, identification, protection, detection, response and recovery, third party risk management and situational awareness. Where material gaps are identified, the institution is expected to formulate a plan to enhance its maturity level; and (iii) Intelligence-led Cyber Attack Simulation Testing ("iCAST") – It is a test of the institution's cyber resilience by simulating real-life cyber attacks from adversaries, making use of relevant cyber intelligence. Institutions with an inherent risk level assessed to be "medium" or "high" are expected to conduct iCAST;

- Professional Development Programme ("PDP"), which seeks to increase the supply of qualified professionals in cybersecurity. In particular, the HKMA has worked with the Hong Kong Applied Science and Technology Research Institute and the Hong Kong Institute of Bankers on the design structure of the PDP; and
- Cyber Intelligence Sharing Platform ("CISP"), which provides an effective infrastructure for sharing intelligence on cyber attacks, and facilitating the timeliness of receiving alerts or warnings in relation to cyber threats. The CISP is operated by the Hong Kong Association of Banks.

Example: in France, financial services providers are required to have in place periodically reviewed internal procedures for risk management, including mitigation measures to protect customers against frauds, scams and illegal usage of personal data. These procedures shall be proportionate to the nature and the complexity of the payment services provided.

53. Policy makers and oversight authorities should ensure that financial services providers monitor threats and vulnerabilities and regularly review the defined risk scenarios (in other words, a cyclical risk management process). They should also ensure the consistent and integrated monitoring, handling and follow-up of security incidents, including security-related customer complaints.

Example: in Hong Kong, under the Supervisory Policy Manual, TM-G-1 General Principle for Technology Risk Management, banks' technology risk management function should formulate a formal technology risk acknowledgement and acceptance process for reviewing, evaluating and approving any major incidents. It should provide support for investigation of any technology-related frauds and incidents. It has to monitor any technology-related issues or incidents regularly.

The HKMA issued a circular in September 2015 related to cyber security risk management. It highlighted the importance of periodic evaluations and monitoring of cyber security risks. The Board should request the senior management to evaluate periodically the adequacy of the AI's cyber security controls, having regard to emerging cyber threats. The HKMA also emphasised that it is crucial to have sufficient cyber security expertise and resources to exercise effective and ongoing checks and balances against monitoring of cyber security controls carried out by the senior management as well as the contingency planning efforts related to cyber attacks.

In addition, in the Cyber Resilience Assessment Framework issued by the HKMA in 2016, it has clear expectations on the cyber incident detection, threat monitoring and analysis, and incident management. For example, policies commensurate with institutions' cyber risk and complexity should be in place to address the concepts of incident response and resilience.

54. Financial services providers should ensure the implementation of sufficiently strong customer authentication mechanisms when contracting a digital financial product or service. This could include exploration of technological innovation to enhance customer authentication and security measures, for example use of two-factor authentication methods.

Example: in France, according to the national provisions transposing PSD2 and the provisions of the EU regulation 2018/389, payment services providers are required to adopt strong customer authentication methodologies based on at least two factors.

Example: in Hong Kong, banks are required to implement two-factor authentication ("2FA") to verify the identity of a customer for high-risk transactions conducted via e-banking services and ensure the ongoing robustness and effectiveness of the implementation of the technologies employed, having regard to emerging cyber threats and fraud risk. During the past years, new customer authentication methods with the use of emerging technologies have been implemented by banks to enhance the security controls and customer experience. For instance, finger vein authentication service was introduced by a retail bank to enhance the customer authentication process for ATM and branch services. Soft token solution was widely adopted for the provision of internet banking services to enhance customer authentication.

Example: in Italy, according to the national provisions transposing PSD2, payment services providers are required to adopt strong customer authentication methodologies based on at least two factors.

Example: Since 14 September 2019, in the European Union, payment service providers (PSPs) must apply strong customer authentication (SCA) where the customer: (i) accesses its payment account online; (ii) initiates an electronic payment transaction; (iii) carries out any action through a remote channel which may imply a risk of payment fraud or other abuses (https://www.bportugal.pt/en/page/strong-customer-authentication).

55. Policy makers and oversight authorities should ensure that financial services providers have in place an effective and convenient process for financial consumers to report unauthorised or fraudulent transactions; any breaches of authentication mechanisms such as passwords; or loss of an access device or token.

56. Policy makers, oversight authorities and financial services providers should consider use of technology, such as SMS messages to issues warnings to clients about identified threats or scams.

Principle 8: Protection of Consumer Data and Privacy

Consumers' financial and personal information should be protected through appropriate control and protection mechanisms. These mechanisms should define the purposes for which the data may be collected, processed, held, used and disclosed (especially to third parties).

The mechanisms should also acknowledge the rights of consumers to be informed about data-sharing, to access data and to obtain the prompt correction and/or deletion of inaccurate, or unlawfully collected or processed data.

Related OECD instruments

The following OECD instruments are relevant:

- OECD Recommendation on Protecting Consumers from Fraudulent and Deceptive Commercial Practices across Borders (2003)
- OECD Privacy Guidelines (2013)
- OECD Consumer Policy Guidance on Mobile and Online Payments (2014)
- OECD Recommendation on Consumer Protection in E-Commerce (2016)
- OECD Recommendation on Artificial Intelligence (2019)

57. Policy makers and oversight authorities should ensure that the legal, regulatory and supervisory framework for financial consumer protection has appropriate safeguards and measures relating to the protection of consumer data and privacy as it relates to transactions with financial services providers, including a definition of "personal data". In some jurisdictions, administration of this framework may be the responsibility of the financial or other national consumer protection or other authorities, in others the responsibility of dedicated personal data protection authorities, or both.

Example: in France, a dedicated authority (Commission nationale de l'informatique et des libertés – CNIL) is dedicated to data and privacy. Legal provisions on financial consumer protection apply without prejudice to the data protection and privacy framework.

Example: in Germany, the Federal Financial Supervisory Authority (BaFin) falls under what is commonly called an "omnibus approach regime": The existing legal framework within the German market defines the functions of different authorities. The role of data protection supervision (according to the General Data Protection Regulation - GDPR and applicable national data protection laws) does not fall within BaFin's mandate. However, in cases where there are specific consumer data protection and privacy risks that apply to the financial industry and that are not covered or inappropriately dealt with in the design and / or the application of the existing data protection laws, BaFin can employ certain measures available within the framework of the supervisory abuse control to sanction supervised entities when systematic irregularities concerning the entities data are found («Missstandsaufsicht»). In all other cases the State Commissioners for Data Protection and Freedom of Information of the federal states (Bundesländer) are responsible.

Example: in Hong Kong, the Office of the Privacy Commissioner for Personal Data ("PCPD") is an independent statutory body established to oversee the enforcement of the Personal Data (Privacy) Ordinance ("PDPO") to protect the privacy of individuals with respect to their personal data. In the handling of customers' personal data, like other data users, banks should comply with the PDPO and relevant codes of practice issued by the PCPD.

As banking supervisor, the HKMA expects banks to ensure a high degree of alertness among their staff members in protecting customer data. Moreover, banks should implement appropriate security controls (covering both IT and non-IT controls) to prevent and detect any loss or leakage of customer data. Various HKMA guidelines and circulars have already covered risk management principles and control measures that are useful for protecting customer data. The HKMA has also from time to time issued circulars to banks reminding them of the need to comply with the provisions of the PDPO in the handling of customers' personal data.

According to the Guideline on Supervision of Stored Value Facility Licensees issued by the HKMA, in respect of any personal data of SVF users (including merchants), a SVF licensee should at all times comply with the PDPO as well as any relevant codes of practice, guidelines or best practice issued by the PCPD from time to time.

Example: in Italy, a dedicated authority for personal data protection has been established. Legal provisions on financial consumer protection apply without prejudice to the data protection and privacy framework.

58. Policy makers and oversight authorities should work with financial services providers to encourage them to (1) make their information collection and use practices transparent and (2) give consumers the ability to make decisions about their data at a relevant time and context.

Example: The HKMA issued a circular on 5 November 2019 to provide banks with a set of guiding principles on consumer protection aspects in respect of the use of big data analytics and artificial intelligence ("BDAI"). These guiding principles focus on four major areas, namely governance and accountability, fairness, transparency and disclosure, and data privacy and protection. The circular requires banks to, among others, (i) provide proper disclosure to customers so that customers could understand banks' approach to using customer data; (ii) ensure that the relevant customer communications are clear and simple to understand; and (iii) carry out appropriate consumer education to enhance consumers' understanding on BDAI technology in banking services.

59. Policy makers and oversight authorities responsible for financial consumer protection should liaise with data protection authorities where they exist to ensure understanding and application of data protection laws and regulations to financial services providers. This could include providing dedicated guidance to financial services providers to promote compliance.

Example: The HKMA organised a briefing session in July 2019 for SVF licensees with the PCPD, during which the Deputy Privacy Commissioner gave an overview of the data ethical framework and shared insights into SVF-related initiatives. Similar briefings will be arranged in future for SVF licensees to develop a better understanding of the requirements and guidelines by the PCPD.

60. Policy makers and oversight authorities should have in place arrangements to cooperate and share information with data protection authorities (where they exist) eg via a memorandum of understanding or through legislative provisions enabling such information-sharing, both at a national and international level.

61. Where data protection laws are administered solely be data protection authorities (ie where the financial consumer protection authority has no oversight), information about breaches of data protection laws should nevertheless be taken into consideration as to the fitness and properness of a financial services provider in meeting their obligations to financial consumers.

62. Financial services providers should implement appropriate policy and adequate internal control measures to ensure compliance with personal data protection regulations and, where relevant, respect consumers' right to personal data privacy. This may include, for example, verifying that mechanisms are in place to safeguard people's personal and financial information and verifying adequate security mechanisms to ensure that financial transactions are protected.

63. Where applicable, financial services providers should ensure that requests for consent to collect, store and use personal data in relation to a financial product or service are clear and understandable in the interests of ensuring informed consent about their data at a relevant time and context. Requests for consent should avoid the use of language or terminology of an overly legal, technical or specialised nature.

> Example: The HKMA issued a circular on 5 November 2019 to provide banks with a set of guiding principles on consumer protection aspects in respect of the use of BDAI. The circular requires banks to, among others, where consent to the collection and use of personal data in relation to a banking product or service powered by BDAI technology is required, ensure that consent is as clear and understandable as possible in the interests of ensuring informed consent.

64. Financial services providers should be responsible for using data only for legitimate purposes and in a manner that serves customers' interests. For example: this can be done for example via a legitimate purposes test, which limits the use of data to what is compatible, consistent, and beneficial to consumers, while allowing firms to use de-identified data to develop new and innovative products and services; and/or via a fiduciary duty requirement, which requires data collection and processing firms to always act in the interests of, and not in ways detrimental to, the subjects of the data.

> Example: the pending Indian Personal Data Protection bill follows both approaches. First, following the fiduciary duty standard, the bill requires that personal data be processed only "in a fair and reasonable manner" that "ensure[s] the privacy of the individual." This element of fairness would make sure that the individual's interests are preeminent. Second, the bill states that data may be used only for the purposes the individual "would reasonably expect that such personal data shall be used for, having regard to the purpose, and in the context and circumstances in which the personal data was collected." In other words, a legitimate purpose standard."

65. Policy makers and oversight authorities should work collaboratively with relevant stakeholders, including other government and regulatory agencies, law enforcement agencies and financial services providers to promote safe online transactions including protection of data privacy.

Example: in Greece, the General Secretariat for Commerce and Consumer Protection collaborates with the Bank of Greece to publicise information to consumers and other stakeholders about new consumer rights deriving from PSD2.

Example: India has a draft personal data protection bill framed as an omnibus law that would create a separate data protection authority. In the past decade, several Asian countries, including the Philippines and Thailand; several African counties, including Ghana, Kenya, Senegal, and South Africa; and several Latin American countries, including Chile and Mexico, have introduced omnibus data protection laws and/or began enforcing them.

66. Policy makers and oversight authorities should explore with financial services providers arrangements that allow consumers to share their financial transaction data with authorised third parties including fintech companies. Privacy and data security concerns should not act as barriers to such innovation, which can promote development of innovative financial management services (such as Open Banking or other financial tools) and in doing so support greater financial inclusion.

67. Policy makers and oversight authorities should monitor financial services providers' use of financial consumer data to develop personalised financial product and service offerings. While such personalisation can support greater tailoring of financial products and services to individual needs, policy makers and oversight authorities should monitor such developments to ensure it does not create the risk of unlawful discrimination or exclusion.

Example: The HKMA issued a circular on 5 November 2019 to provide banks with a set of guiding principles on consumer protection aspects in respect of the use of BDAI. The circular requires banks to, among others, ensure that (i) the BDAI model complies with the applicable laws, including those relevant to discrimination; and (ii) customer access to basic banking services are not denied unjustifiably which will be against the spirit of financial inclusion.

68. Policy makers and oversight authorities should ensure financial services providers have robust and transparent governance, accountability, risk management and control systems relating to use of digital capabilities (such as AI, algorithms and machine learning technology). This includes ensuring that the methodology of algorithms underpinning digital financial services (eg digital financial advice) is clear, transparent, explainable and free from unlawful and exclusionary biases, and with options for recourse where necessary. This entails providing easy-to-understand information to people affected by algorithms underpinning digital financial services that can enable those adversely affected by the outcome to be able to challenge it.

For example, the OECD Recommendation on Artificial Intelligence (2019) includes a Principle on Transparency and explainability, in accordance with which those who play an active role in the AI system lifecycle, including organisations and individuals that deploy or operate AI should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

a. to foster a general understanding of AI systems,

b. to make stakeholders aware of their interactions with AI systems, including in the workplace,

c. to enable those affected by an AI system to understand the outcome, and,

d. to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

Example: privacy representatives, whether persons or digital mechanisms, could be introduced to assess decision-making models for fairness, bias and exclusion. This can serve as a critical tool to prevent exclusion as products are introduced that use AI and machine learning to assess who is eligible and on what terms products are introduced.

Example: In Hong Kong, considering that the growing use of artificial intelligence presents not only opportunities but also new risk management challenges to banks, the HKMA issued a circular on 1 November 2019 to set out a set of high-level principles as guidance to the banking industry. These principles cover areas such as governance, application design and development and on-going monitoring and maintenance. Banks may apply these principles in a proportionate manner that reflects the nature of their artificial intelligence applications and the level of risks involved.

The HKMA further issued a circular on 5 November 2019 to provide banks with a set of guiding principles on consumer protection aspects in respect of the use of BDAI. These guiding principles focus on four major areas, namely governance and accountability, fairness, transparency and disclosure, and data privacy and protection. The circular requires banks to, among others, (i) ensure that BDAI models produce objective, consistent, ethical and fair outcomes to customers; (ii) provide appropriate level of transparency to customers regarding their BDAI applications through proper, accurate and understandable disclosure (including, make clear to customers prior to service provision that the relevant service is powered by BDAI technology and of the associated risks, provide explanations on what types of data are used and what factors or how the models affect the BDAI-driven decisions, etc.); (iii) make available a mechanism for customers to enquire and request reviews on the decisions made by BDAI applications, and ensure that any related complaint handling and redress mechanism for BDAI-based products and services are accessible and fair; (iv) have the board and senior management remain accountable for all the BDAI-driven decisions and processes, and accordingly they should ensure appropriate governance, oversight and accountability framework which is established and documents; and (v) ensure appropriate level of explainability of the BDAI models including any algorithms (i.e. no black-box excuse) and that the models can be understood by banks.

69. Oversight authorities should ensure they have the technological capability, resources and tools to be able to oversee and understand the digital capabilities being deployed by financial services providers. These capabilities could be developed in-house or could be outsourced to a different public authority within the jurisdiction that can provide the necessary expertise.

70. Policy makers and oversight authorities should ensure that financial services providers that use automated decision-making models such as credit scoring, ensure that they take measures to mitigate against irresponsible or inappropriate outcomes, such as automatic refusals. Measures could include appropriately weighting all the relevant variables and providing for human intervention, where appropriate.

Example: The HKMA issued a circular on 5 November 2019 to provide banks with a set of guiding principles on consumer protection aspects in respect of the use of BDAI. The circular requires banks to, among others, ensure (i) the models used for the BDAI-driven decision are robust and have appropriately weighed all relevant variables; (ii)

the possibility of manual intervention to mitigate irresponsible lending decisions where necessary.

71. Financial services providers should consider embedding personal data protection into the design of a financial product or system at the outset (i.e. "privacy by design") including use of privacy-friendly default settings, and/or collecting and storing only the minimum amount of personal data for the minimum amount of time (i.e. "data minimisation").

Example: In Hong Kong, the Office of the Privacy Commissioner for Personal Data ("PCPD") has published some good practices on Fintech and BDAI. These include, among others, the "Ethical Accountability Framework" and the "Data Stewardship Accountability, Data Impact Assessments and Oversight Models" and the "Information Leaflet on Fintech". The HKMA has engaged with the PCPD in Hong Kong to provide more guidance to the banking industry on the proper use of personal data in the online environment. In particular, the HKMA has organised a seminar in April 2019 and invited the Privacy Commissioner for Personal Data in Hong Kong to share with the industry a number of good practices including the adoption of "privacy by design" and "privacy by default" when developing fintech initiatives. The HKMA supports the concept of data ethics and stewardship in the context of collecting and using personal data, and issued a circular on 3 May 2019 to encourage banks to adopt and implement the Ethical Accountability Framework issued by the PCPD in Hong Kong. In addition, according to the circular issued by the HKMA on 5 November 2019 regarding consumer protection aspects on the use of BDAI, banks are required to consider embedding data protection in the design of a product or system from the outset (i.e. "privacy by design") and collecting and storing only the minimum amount of data for the minimum amount of time (i.e. "data minimization").

Principle 9: Complaints Handling and Redress

Jurisdictions should ensure that consumers have access to adequate complaints handling and redress mechanisms that are accessible, affordable, independent, fair, accountable, timely and efficient. Such mechanisms should not impose unreasonable cost, delays or burdens on consumers.

In accordance with the above, financial services providers and authorised agents should have in place mechanisms for complaint handling and redress (i.e. internal complaints procedures). Recourse to an independent redress processes should be available to address complaints that are not efficiently resolved via the internal dispute resolution mechanisms.

At a minimum, aggregate information with respect to complaints and their resolutions should be made public.

72. Oversight authorities should ensure that the requirements on complaints handling and redress apply equally to all providers of financial products or services, irrespective of the distribution channel used.

> Example: in Portugal, consumers have the right to lodge a complaint about credit institutions, financial companies, payment institutions, electronic money institutions or credit intermediaries in the retail banking markets (bank deposits, mortgage credit, consumer credit, payment services, etc.), free of charge, using for example the Complaints Book, in the physical or digital format. Complaints can be lodged regardless of the channel used to contract a financial product or service. Customers may also present those complaints directly to the Central Bank of Portugal, through the Bank Customer Website (www.clientebancario.bportugal.pt/formulario-nova-reclamacao) – Banco de Portugal's dedicated website to provide information to consumers and the industry – or written communication (e-mail, letter of fax). This means there is direct and mandatory involvement of the supervisory authority in the analysis of all these complaints, which is also used as a tool to monitor the conduct of supervised institutions and to define supervisory initiatives.
>
> Example: in Spain, Banco de España handles claims and complaints made by consumers against entities supervised by Banco de España, arising from alleged non-compliancecompliance with regulations on transparency and protection of customers or of good financial practices, in order to secure their interests and rights. Claims and complaints may be made free of charge. Likewise, complaints can be lodged regardless of the channel used to contract a financial product or service. The Banco de España periodically publishes statistics on this matter, through its Department of Market Conduct and Claims.
>
> Example: in Germany, collective consumer protection is one of BaFin's core tasks. BaFin offers various means of assistance to consumers. They can complain with BaFin about any supervised company. Complaints can be submitted in various ways (letter, fax, e-mail or online complaints form).
>
> In the area of investment advice and portfolio management, the service providers have to report to BaFin not only all their staff tasked with provision of these services, but also each customer complaint regarding the provision of these services. That way, BaFin gains valuable information on how complaint handling processes work within the supervised entities, and is able to scrutinize the handling

of single complaints too. As a positive side effect, the reporting obligation has a significant disciplining effect on the supervised institutions.

These measures ensure that the necessary complaint handling procedures are observed by all relevant market participants, regardless of the technology behind the service or the communication channel.

73. Consumers should be given clear and precise information on the right to complain and on the procedures to be followed to make a complaint when contracting a financial product or services through digital means. This could mean, for example, prominent and easy-to-follow links via a homepage, FAQs or mobile app menu to the complaints procedure and/or an external redress process.

Example: in Portugal, when contracting a consumer credit, a mortgage credit, a deposit or a payment service, regardless of the distribution channel used, credit institutions (and, in some cases, credit intermediaries) are required to provide pre-contractual information, containing information on the right to complain.

Example: the Bank of Italy provisions on financial consumer protection require banks and other financial institutions granting credit to provide consumers, before entering into the contract, with information on the right to complain and on the procedures to be followed to make a complaint when contracting a financial products or services, even when they are offered through digital means.

Example: in Spain, institutions that grant credit to consumers must provide them with the European Standardised Information Sheet, containing the contact details of the complaint service and ADR mechanisms (Law 16/2011, of June 24).

74. Complaints handling and redress mechanisms should be capable of dealing with new types of complaint which may arise from the provision of digital financial services e.g. account hacking, compromised account security or mistaken payments.

Example: in Germany, BaFin has published supervisory guidance on complaints handling in the three sectors (banking, insurance, securities). These guidelines are structured around a very broad definition of complaint: "Any utterance of discontent related to the provision of financial services". This broad definition was chosen expressly in order to encompass every possible type or reason of complaining, while simultaneously ruling out complaints that do not relate to supervised business (i.e. concerning the condition of physical branches or the lack of parking space).

75. Complaints should be accepted by digital means (website, e-mail, text, live-chat etc), where firms are also using these media to provide services, as well as more traditional means like post or phone.

Example: in Hong Kong, banks are required to have in place appropriate management controls and take reasonable steps to handle complaints fairly, consistently and promptly. Among others, banks should clearly communicate to customers about where and how to complain, for example, to publish details of their internal complaint handling procedures on their websites and to allow complainants to make a complaint by any reasonable means, such as letter, telephone, facsimile, e-mail or in person.

The HKMA, as a bank regulator, publishes a full list of banks' contact persons for handling customer complaints on its website

(https://www.hkma.gov.hk/media/eng/doc/other-information/Banks_contact_persons.pdf) which provides the public easy access to the banks' complaint channels and gives the bank concerned a chance to resolve the complaint at an early stage. A dedicated page has also been set up in the website of the HKMA to provide the public with information on FAQs, animation video and flowchart on its complaint handling process, together with a complaint form for download. The completed complaint form could be sent back to the HKMA by post, facsimile, e-mail or in person.

Telephone enquiry is one of the most popular ways of communication in Hong Kong. As such, the HKMA and all retails banks have set up complaint hotline or telephone enquiry services for the public to get in touch with them easily. With the advancements in information technology and the prevalence of the Internet, an Electronic Complaint Form will also be available in late 2019 allowing bank customers to lodge their complaints against banks through the HKMA website directly.

Example: in Portugal, all providers of goods and services, including financial institutions, are required to make available a Complaints Book at each branch. Decree-Law no. 74/2017 established the ability for citizens to file complaints through an electronic platform, called "Complaints Book Electronic" (available at www.livroreclamacoes.pt/inicio – this link can be found at the financial services providers' websites). It provides the specific forms for information requests and complaints, and forwards the latter to the entity complained about and to the competent supervisory authority, enabling the tracking of the status of the complaints and allowing the production of statistical data. Customers may also present those complaints directly to the Central Bank of Portugal, through the Bank Customer Website (www.clientebancario.bportugal.pt/formulario-nova-reclamacao).

Example: Spanish Ministerial Decree ECO/734/2004, of March 11, extends to contracts signed by telematic means the obligation of financial institutions to inform on their website of the existence of a customer service department, as well as its email and postal address. It also requires these entities to facilitate the filing of complaints through electronic means.

Example: in Germany, the supervised entities are required to accept and handle customer complaints regardless of the communication channel

76. The needs of vulnerable groups should be considered when designing and publicising the complaints process.

Example: banks in Hong Kong are expected to provide special assistance to customers with disability or language problems for making a complaint. The HKMA will also provide assistance to persons in need to fill in the complaint form.

Example: in Japan, according to the "Comprehensive Guidelines for Supervision", financial firms are expected to develop a control environment wherein they extensively publish contact points and ways of making applications, and which are made known to customers in a way that is easy for them to understand and which also take into account their diversity.

77. Consumers should be informed about and have access to ADR services regardless of the channel used to contract a financial product or service.

Example: for complaints involving monetary disputes, banks in Hong Kong are expected to inform their customers about their rights to refer the matter to the Financial Dispute Resolution Centre ("FDRC"). Through its website (https://www.fdrc.org.hk/), leaflets, hotline and social media, the FDRC explains to the public about the possible channels to resolve their monetary disputes with banks through mediation and/or arbitration.

Example: in Italy, for disputes concerning banking and financial transactions and services, including payment services, consumers are informed about their right to lodge a dispute with the Banking and Financial Ombudsman both by the means provided by the Bank of Italy and by the intermediaries. Easy-to-follow practical information about this ADR scheme and how to access it is available on the Ombudsman's website (available in Italian and in English), on social media (Youtube channel, Twitter, LinkedIn, Storify), and in the Bank of Italy's Annual Report on the activity of the Ombudsman, available on the abovementioned website) With reference to intermediaries, consumers are appropriately informed mostly through the transparency documentation.

According to the Italian legislation (Legislative Decree 28/2010), recourse to the Ombudsman satisfies the pre-condition for filing a judicial proceeding: those who want to commence a civil proceeding may complain to the Ombudsman as an alternative to mediation. Consumers have access to the ADR regardless of the channel used to contract the product or service. Proceedings conducted by the Banking and Financial Ombudsman are free of charge for consumers.

Example: in Portugal, institutions that provide mortgage and consumer credits, payment accounts (including those with basic features) payment services and credit intermediaries' services are required to provide effective and adequate ADR mechanisms. To this end, these institutions must be covered by at least two alternative dispute resolution entities that are part of the consumer arbitration network, as disclosed on the Bank Customer Website.

Example: in Spain, firms trading and providing online services to customers must include on their websites a visible and easy accessible link to the Online Dispute Resolution (ODR) platform set by Regulation (EU) N.º 524/2013 and aimed at resolving disputes between consumers and traders in the EU or Norway, Iceland and Liechtenstein carrying out domestic or cross-border online transactions.

Example: in Germany, financial service providers are required to inform their clients about their possibilities of ADR, the responsible ADR entity and about whether the company is willing to participate in ADR or accept an ADR decision. Additionally or alternatively, consumers can also address their complaints to private and official ombudsmen schemes generally free of charge.

BaFin also runs an official consumer dispute resolution entity, the Arbitration Board, pursuant to section 14 (1) of the German Injunctions Act (Unterlassungsklagegesetz- UKlaG). It is responsible for the out-of-the court resolution of consumer disputes related to investment funds and banking service providers. The Arbitration Board at BaFin is designed as a substitute dispute resolution entity for financial services, meaning it is only responsible if there is no recognized private consumer dispute resolution entity. Proceedings conducted by the arbitration board at BaFin are free of charge for consumers. However, expenses such as postage or costs of legal counsel are not reimbursed. Consumers

do not necessarily have to be represented by a third party (such as a lawyer) in the arbitration proceedings, however. The arbitrators are qualified to hold judicial office and are employed by BaFin. They have several years of legal professional experience. As arbitrators, they are independent and not subject to instructions

78. Complaints to ADR services should be able to be made by digital means, as well as by other means.

Example: in Italy, according to the principles provided for by the ADR Directive 2013/11/EU on alternative dispute resolution (ADR), consumers can file their complaints with the Banking and Financial Ombudsman via a web portal, operational from February 2018. The web portal is a simple and interactive tool that assists users in filing a complaint through a specific guided procedure and allows users to manage the whole procedure, to verify the status of their complaints and to receive the defence briefs from the intermediaries and the Ombudsman's decisions. At a later stage the Portal will be accessible also to intermediaries and their association to interact directly with the complainants and the Bank of Italy's technical secretariats, which support the Ombudsman's activities. Without prejudice to the full decision-making autonomy of the Ombudsman, the Bank of Italy's technical secretariats may assist customers in the complaints' submission phase.

Example: in Spain, Ministerial Decree ECO/734/2004, of March 11, requires financial institutions' customer service to submit to their board of directors or equivalent body an annual report containing statistical data and suggestions based on the information gathered through the complaints handling in order to better achieve their objectives.

Example: the Central Bank of Portugal, under its oversight mandate, uses complaints as a tool for retail banking market supervision and to ensure consumer protection. In particular, it assesses the supervised institutions' compliance with laws and regulations when providing financial products and services in order to increase consumer confidence in the market and its quality standards. The central bank publishes data on complaints on a half-yearly basis (report on Banking Conduct Supervision Activities and Banking Conduct Supervision Report). Institutions are ranked by number of complaints received about them (considering a weighted average of the number of payments accounts, of credit agreements or mortgage credit agreements, for example). Furthermore, the Central Bank of Portugal publishes the number of specific determinations and recommendations or the number of administrative proceedings that are initiated for breaches of the law or regulations according to the complaints' classification (for example, number of specific determinations and recommendations on mortgage credit and the number of institutions subject to measures in a given year).

79. Firms should collect and analyse complaints data in order to identify and address recurring or systemic problems and learn lessons in terms of digital financial products, services or processes.

Example: in Ireland, regulated entities are required to undertake an appropriate analysis of the patterns of complaints received from consumers on a regular basis (and at least on an annual basis), including investigating whether complaints indicate an isolated issue or a more widespread issue for consumers. This analysis of consumer complaints must be escalated to the regulated entity's

compliance/risk function and senior management. [Provision 10.12 of the Central Bank of Ireland's Consumer Protection Code 2012]. Where a regulated entity providing financial services within Ireland fails to comply with the Central Bank's Consumer Protection Code – including in respect of the Code's perspective consumer complaints handling provisions - the Central Bank has the power to administer sanctions (under Par IIIC of the Central Bank Act 1942).

Example: in Spain, Ministerial Decree ECO/734/2004, of March 11, requires financial institutions' customer service to submit to their board of directors or equivalent body an annual report containing statistical data and suggestions based on the information gathered through the complaints handling in order to better achieve their objectives.

80. Firms that use computer programmes or algorithms in the dispute resolution process should ensure that they are robust, appropriately weight all relevant variables and where necessary, provide the possibility of human intervention in complex or contested disputes. Firms should ensure that such algorithms produce outcomes which are objective, consistent and fair for financial consumers.

81. Oversight bodies should ensure they are regularly provided with, and have access to, information about complaints against financial services providers. Such information is valuable for supervisory purposes, including monitoring trends and risks in relation to digital financial services (e.g. security issues).

Example: the Bank of Italy collects information on an annual basis about complaints addressed to banks and other supervised intermediaries, included their number, status (whether accepted, rejected or still to be handled) and objective. Information about complaints is taken into account by supervisory processes.

Example: Germany: BaFin runs a special, free-of-charge, consumer helpline. The helpline staff answer consumers' questions or explain the measures available if consumers want to settle a conflict out of court with financial service entities. As a special service, there is a sign language phone service for the deaf and people with hearing difficulties. The consumer helpline offers also "co-browsing", a feature that allows consumer helpline advisers to navigate websites together with callers.

The consumer helpline, as well as the general customer complaints received by BaFin, also act as an early warning system for the BaFin supervisory divisions, especially in the event of critical situations on the financial markets. BaFin usually asks the company for a statementto the customer complaint and receives further information that way. Complaints provide BaFinwith an important source of information for its supervisory work. They alert BaFin to cases where review is needed whether a company is taking its responsibilities seriouslyand whether supervisory measures are necessary. Complaints can also reveal structural weaknesses in a company.

In addition, in the insurance sector, BaFin obtains annual complaints reports from the supervised entities, containing the number of complaints received (total number and broken down by class of insurance) during the last year, a summary of the resolution status and processing time of each complaint, an overview of the different complaint causes and number thereof in each case, statements on the number of complaints from each complainant that have been successful, at least partially, during the reporting period.

Example: the Central Bank of Ireland has been collecting detailed consumer data from selected regulated firms in a number of financial services sectors since 2013. This reporting allows for the identification of potential risks to the Central Bank's consumer protection objectives as well as the analysis of market trends and movements. Included in this bi-annual reporting is data relating to complaints received by financial services providers from consumers. In addition, the Central has a close working relationship with the Financial Services and Pensions Ombudsman who provides information on patterns of complaints that it deems as warranting the Central Bank's supervisory attention or any specific complaints queried.

Example: in Japan, the FSA has a "Counselling Office for Financial Services Users" that responds to general questions or complaints, to requests and feedbacks from financial service customers concerning financial administration and financial services. Expert counsellors respond to the questions and the requests by phone. Furthermore, the feedback from the customers is shared with the supervision bureau in the FSA and used for the purpose of promoting customer protection. The Office cannot mediate or accommodate a dispute, but introduces advisors in institutions, as appropriate, for resolution, or summarizes the issue based on advising activities.

Example: according to the Portuguese law, there is a mandatory involvement of the supervisory authority in the analysis of complaints: every citizen has the right to lodge a complaint, free of charge, with Banco de Portugal, using for example the Complaints Book or directly at the Bank Customer Website. The Central Bank of Portugal uses complaints as a tool for retail banking market supervision and to ensure consumer protection. Complaints allow a cross-market analysis that may reveal a need for regulatory intervention or the development and implementation of financial literacy programmes for bank customers. The information collected through complaints when combined with other supervisory tools, such as on- and off-site inspections, may lead to a more focused and detailed analysis of a particular segment of supervised matters. The central bank publishes data on complaints, in particular regarding their main subjects, ranks the institutions by the number of complaints regarding each subject, the complaint's status and the analysis result.

Example: Banco de España prepares half-yearly a report to the Ministry of Economy based on the complaints received. If the processing of complaints reveals any sign of punishable conduct, this information is transferred to the supervision department (Ministerial Decree ECC/2502/2012). Since the adoption by Banco de España of EBA Guidelines for complaints handling on 29 October 2014, this oversight body ensures that supervised entities analyse, on an ongoing basis, complaints-handling data, to guarantee that they identify and address any recurring or systemic problems, and potential legal and operational risks.

82. Use of digital means for complaints procedures should be used to facilitate the collection, aggregation and publication of complaints data.

Example: in Italy, banks and financial institutions are required to report on their website the results of their complaints handling procedures and the related data. As far as redress procedures are concerned, information about the Ombudsman's activities is made available to the public through the Annual Reports available on the Ombudsman's website. In addition, the outcomes of the Ombudsman's

proceedings make a significant contribution to the supervision of the banking and financial system; according to the Ombudsman's Provisions, the decisions become part of the broader pool of information at the Bank of Italy's disposal for its regulatory and supervision functions. .

Example: the Central Bank of Ireland uses social and online media monitoring services from a third party provider to provide a greater understanding of how firms are treating consumers, consumer attitudes towards firms, key sectoral trends, and launches of new products/services and FinTech offerings. Social media therefore provides the Central Bank with a valuable resource to understand consumers' experiences and concerns about financial services and products in real-time.

Example: Banco de España publishes the "Annual Claims Report" annually through its web page. This report provides a statistical analysis of the proceedings processed indicating, amongst other things, the areas in which claims and complaints were lodged, as well as the relevant entities. The report also indicates the transparency regulations and the best practice criteria applied in the resolutions issued during the corresponding year.

Example: the Central Bank of Portugal also provides the possibility of a bank client to lodge a complaint directly to the central bank using the Bank Customer Website. Moreover, bank clients may complain using the electronic complaints book, a platform that allows clients to lodge a complaint electronically, also free of charge. With the information collected, the central bank publishes data on complaints on a half-yearly basis (report on Banking Conduct Supervision Activities and Banking Conduct Supervision Report).

83. Given the increasingly cross-border nature of the provision of financial services facilitated by digital channels, the following should be taken into consideration in terms of effective complaints handling and redress mechanisms:

- Consumers should be given clear information on the relevant jurisdiction in relation to a cross-border financial product or service offered through digital channels.
- Oversight bodies and ADR services from different jurisdictions should cooperate and exchange information to ensure that adequate complaint handling and redress mechanisms in relation to the cross-border provision of products or services through digital means.

  Example: in Italy, at the Banking and Financial Ombudsman, a specific section providing for information on the Fin-Net network and on the cross-border complaints handling is available to customers into the Ombudsman's website. A consumer that wants to file a complaint against a foreign intermediary that is subject to a foreign out-of-court settlement scheme which is a member of Fin-Net, can contact the Italian Ombudsman for support.

  Example: in Germany, the BaFin Arbitration Board is also member of FIN-NET and can forward an application to the responsible dispute resolution scheme of FIN-NET if necessary. Within FIN-NET, the schemes cooperate to provide consumers with easy access to out-of-court complaint procedures in cross-border cases, if they do not want to take a cross-border dispute to court.