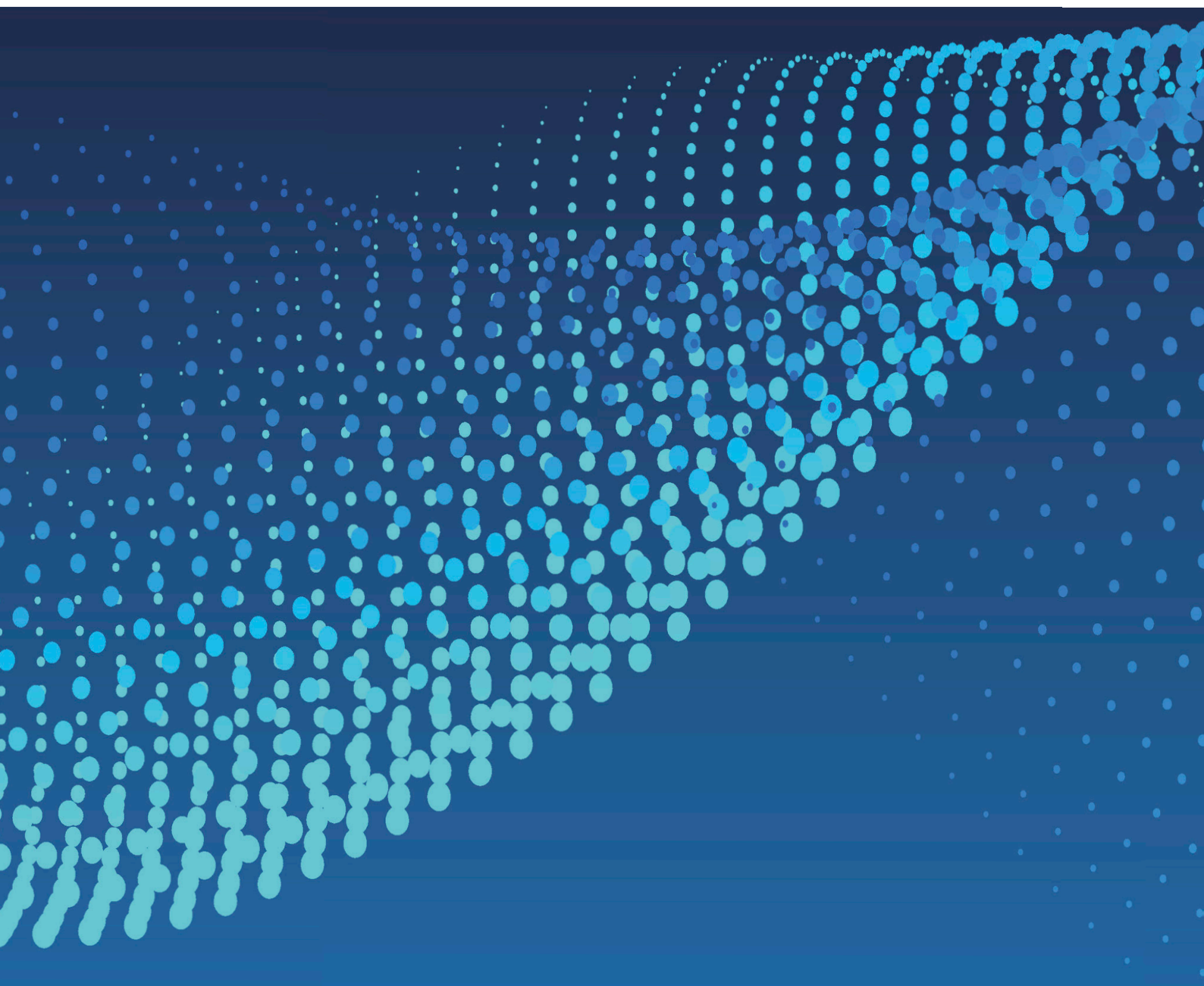


G20/OECD Policy Guidance

Financial Consumer Protection Approaches in the Digital Age



Please cite this publication as:

OECD (2018), G20/OECD Policy Guidance on Financial Consumer Protection Approaches in the Digital Age

This work is published under the responsibility of the Secretary-General of the OECD. The opinions expressed and arguments employed herein do not necessarily reflect the official views of OECD member countries.

This document and any map included herein are without prejudice to the status of or sovereignty over any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

Foreword

Given the increasingly digital environment for financial products and services and the potential for digitalisation to support greater financial inclusion and inclusive growth, the need for effective financial consumer protection is more important than ever. It is equally important that the policies and approaches developed and adopted by financial consumer protection authorities need to evolve and adapt in line with the environment.

This policy guidance is for consideration by policy makers responsible for the implementation and application of key elements of the G20/OECD High-Level Principles on Financial Consumer Protection in a digital environment and G20 High-level Principles on Digital Financial Inclusion with respect to principle 5. It focuses on areas related to the role of oversight bodies and disclosure and transparency.

This policy guidance has been developed by the G20/OECD Task Force on Financial Consumer Protection. Building on the report on digitalisation and financial inclusion delivered under Germany's G20 presidency, this note contributes to the priorities of Argentina's G20 presidency.

Following an extensive consultation process with members of the Task Force, the Global Partnership for Financial Inclusion (GPFI) and other stakeholders, the note was approved by the Task Force and the OECD Committee on Financial Markets in May 2018 and endorsed by the GPFI in June 2018. It is now transmitted to the G20 Finance Ministers and Central Bank Governors at their meeting in Buenos Aires on 19-20 July 2018.

This document is complemented by G20/OECD INFE Policy Guidance on Digitalisation and Financial Literacy. It contributes to the OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.

Contents

FOREWORD.....	3
INTRODUCTION	5
POLICY GUIDANCE ON FINANCIAL CONSUMER PROTECTION APPROACHES IN THE DIGITAL AGE	9
Rationale	9
Policy context.....	10
G20 High Level Principles for Digital Financial Inclusion (DFI Principles).....	10
G20/OECD Task Force on Financial Consumer Protection and High Level Principles on Financial Consumer Protection (FCP Principles)	10
Background	12
Benefits of digital financial services	12
Risks of digital financial services	13
Objectives and Scope	14
Overarching considerations	15
Oversight arrangements and capability.....	15
Disclosure and Transparency	24
REFERENCES	29

Introduction

Supporting digital financial inclusion, and the concurrent need for appropriate and relevant financial consumer protection, as well as strengthened digital financial literacy, has been highlighted as a priority for the Argentinian G20 Presidency, building on the work of the Chinese Presidency in 2016 and continuing with the German Presidency in 2017.

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, the G20/OECD Task Force on Financial Consumer Protection (“the Task Force”)¹ has committed, via its Programme of Work, to develop policy guidance for consideration by policy makers responsible for the implementation and application of key elements of the G20/OECD High-Level Principles on Financial Consumer Protection (“the FCP Principles”) in a digital environment. This is the first such Policy Guidance Note produced by the Task Force. It is focussed on two of the FCP Principles (relating to the role of oversight bodies and disclosure and transparency) and is likely to be supplemented by further guidance addressing the remaining FCP Principles and as more approaches are developed to protecting the interests of financial consumers in the digital environment.

The development of this Policy Guidance Note is based on input of Task Force members about the practices and approaches that are being adopted or trialled in different jurisdictions. The Policy Guidance is flexible, non-binding and designed to support jurisdictions to learn from each other and share insights.

This Policy Guidance Note supports the implementation of Principle 5 of the G20 High Level Principles for Digital Financial Inclusion (“the DFI Principles”) published by the GPFI. This principle relates to the need for jurisdictions to establish responsible digital financial practices to protect financial consumers and build trust and confidence in digital financial services, by establishing a tailored approach to financial consumer protection that focuses on issues of specific relevance to digital financial services. The OECD is an implementing partner of the GPFI subgroup on Financial Consumer Protection and Financial Literacy.

¹ The G20/OECD Task Force on Financial Consumer Protection was established in 2010 as part of the strategic response to the financial crisis to conduct financial consumer protection policy and research on behalf of the G20 and the OECD. The Task Force comprises members from G20 and OECD economies, with policy, analytical and secretariat support from the OECD. Among other things, the Task Force is responsible for the G20/OECD High Level Principles on Financial consumer Protection, which set out a comprehensive framework for enhancing financial consumer protection.

This Policy Guidance Note is complemented by a Policy Guidance note on Digitalisation and Financial Literacy, developed through the OECD/International Network on Financial Education (INFE), which addresses the implementation of Principle 6 of the G20 High Level Principles for Digital Financial Inclusion.

Both Policy Guidance Notes contribute to the content of a Policy Guide compiled by Argentina's G20 Presidency: *Digitisation and Informality: G20 Policy Guide to Harness Digital Financial Services to Individuals and MSMEs in the Informal Economy*.²

Process

This Policy Guidance Note has been produced by the OECD based on inputs from members of the Task Force via an iterative and consultative process. It also takes account of discussions held during Task Force meetings and consultation with key stakeholders, including relevant international organisations and standard setting bodies. It has been reviewed and approved by the OECD Committee on Financial Markets (CMF). It has also been shared with members of the Global Partnership on Financial Inclusion (GPFI) for review and comments.

This Policy Guidance Note incorporates comments and feedback from Task Force members and from GPFI members, implementing partners and other stakeholders.³

The Policy Guidance Note was approved in May 2018 by the Task Force and its parent body, the OECD Committee on Financial Markets and endorsed by the GPFI in June 2018. It is now transmitted to the G20 Finance Ministers and Central Bank Governors.

² *Digitisation and Informality: a Policy Guide to Harness Digital Financial Services for Individuals and MSMEs in the informal economy*, GPFI, 2018

³ Comments and feedback were received from Argentina, Brazil, Canada, France, Germany, Hong Kong China, Ireland, Italy, Japan, Luxembourg, Portugal, United Kingdom, United States, CGAP, European Union, IAIS, IOSCO, the World Bank and the World Economic Forum.

Policy Guidance on Financial Consumer Protection

Approaches in the Digital Age

Rationale

Digital technologies are increasingly integrated in the economy and are making a significant impact in the financial services industry by introducing new products, services, distribution models and providers. Digitalisation is affecting individuals and businesses globally, with mobile money services now available in 64% of developing countries, and their spread is likely to increase hand-in-hand with the growing penetration rate of mobile connections (estimated to exceed 100% by 2020).⁴ These significant changes underline the need for effective financial consumer protection, financial education and financial inclusion policies that adapt to this changing environment.

As noted by Consumers International in their 2017 report *Banking on the Future*, consumers stand to benefit from the digitalisation of finance (“the age of fintech”) in terms of increased competition and the gain in choice, service and value that will follow and increased access to financial services for groups of consumers for whom such services had previously been out of reach, or sub-optimal.⁵ These benefits can be substantial for consumers worldwide, and offer significant opportunities to integrate the poor and the financially excluded populations in the formal financial sector.⁶

The digitalisation of finance is accompanied by vastly and rapidly increasing levels in the generation, collection, storage, sharing and use of personal and transactional data enabled by digital technology (including “big data”), which includes data collected through mobile or online interactions, but also increasingly by a wide range of other applications. For example, according to a study by IDC Digital Universe, worldwide data storage is forecast to reach 40 zettabytes⁷ by 2020 and increase 50-fold from the beginning of 2010 to the end of 2020.⁸

⁴ *State of the Industry Report Mobile Money*, GSMA, 2015.

⁵ *Banking on the Future, an exploration of fintech and the consumer interest*, Consumers International, July 2017

⁶ According to a McKinsey study, referenced in the report of the Responsible Finance Forum VIII 2017, digital finance could increase the gross domestic product of emerging economies by 6 percent, or a total of US\$3.7 trillion by 2025.

⁷ A zettabyte is a multiple of the unit byte for digital information. The prefix zetta indicates multiplication by the seventh power of 1000 or 10^{21} in the International System of Units (SI). A zettabyte is one sextillion (one long scale trillion) bytes

⁸ *International Data Corporation Digital Universe Study: Big Data, Bigger Digital Shadows and Biggest Growth in the Far East*, December 2012

Policy context

In order to both better realise the benefits of digital financial services, and to mitigate the risks, policy makers and relevant private and civil stakeholders, should take concrete actions which include establishing and complying with appropriate and flexible financial consumer and data protection frameworks, complemented by efforts to strengthen the digital and financial literacy of consumers.

This Policy Guidance Note builds on and supports the implementation of existing policy instruments, in particular those set out below.

G20 High Level Principles for Digital Financial Inclusion (DFI Principles)

The DFI Principles were produced in 2016 by the Global Partnership for Financial Inclusion (GPFI), under the Chinese Presidency of the G20.⁹ The DFI Principles are intended to drive the adoption of digital approaches to achieve financial inclusion goals, as well as the related G20 goals of inclusive growth and increasing women's economic participation. The DFI Principles are focussed on the need to provide the financially excluded and underserved with high-quality and appropriate financial products and services and the potential to use digital technologies to achieve this goal, where possible. Importantly, the DFI Principles reflect the fact that access to financial services alone is insufficient. Rather, fostering widespread usage and understanding of responsible digital financial services is critical to individual, national and global welfare. The DFI Principles also recognize the need to actively balance the promise of digital innovation with the new risks that rapidly evolving technology introduces.

While the DFI Principles provide a holistic basis for action by jurisdictions to promote digital financial inclusion, DFI Principle 5 relates specifically to the need for responsible digital financial practices to protect consumers and a comprehensive approach to consumer and data protection that focuses on issues of specific relevance to digital financial services.

G20/OECD Task Force on Financial Consumer Protection and High Level Principles on Financial Consumer Protection (FCP Principles)

The Task Force was established in 2010 in response to the financial crisis and in recognition of the fact that appropriate financial consumer protection – together with access to appropriate financial products and good quality financial education – are fundamental requirements for consumer trust and confidence in the market.

The Task Force is responsible for the FCP Principles, first endorsed by the G20 in 2011.¹⁰ The Principles are designed to assist policy makers in developing comprehensive financial consumer protection frameworks. They are widely acknowledged and their implementation is monitored by the Task Force on an ongoing basis. The Principles cover the following areas:

- The legal, regulatory and supervisory framework underpinning financial consumer protection

⁹ G20 High Level Principles for Digital Financial Inclusion, 2016, GPFI

¹⁰ G20/OECD High Level Principles on Financial Consumer Protection, October 2011, OECD

- The role of oversight bodies (i.e. public authorities with the mandate for financial consumer protection)
- Equitable and fair treatment of consumers
- Disclosure and transparency
- Financial education and awareness
- Responsible business conduct of financial services providers and authorised agents
- Protection of consumer assets against fraud and misuse
- Protection of consumer data and privacy
- Complaints handling and redress
- Competition

The Principles are supported by relevant, practical and evidence-based guidance and examples about how they can be implemented by policy makers in the form of Effective Approaches.¹¹ These Effective Approaches reflect the different ways that jurisdictions have implemented the Principles. In this way, the Effective Approaches provide suggested actions or a “tool box” of policy options on how to enhance financial consumer protection.

The Effective Approaches consist of:

- *Common Effective Approaches* which are considered by the Task Force to effectively implement particular aspects of the Principles and have been adopted or applied by a broad range of jurisdictions, and
- *Innovative or Emerging Approaches* which are not necessarily representative across a broad range of jurisdictions but instead may be limited to only a few jurisdictions and sometimes are only applied to certain financial services. The Task Force considers that, after taking into account specific national circumstances, these innovative or emerging approaches can be of interest to and prove useful for stakeholders engaged in work to enhance financial consumer protection.

Together, the DFI Principles and the FCP Principles constitute the foundation of the work of the GPFI subgroup on financial consumer protection and financial literacy relating to financial consumer protection, and can serve as a solid and broad policy basis to develop further policy tools and in particular implementation guidance relevant to technology and digital aspects.

¹¹ Update Report on the Work to Support the Implementation of the G20 High Level Principles on Financial Consumer Protection Principles 4, 6 and 9, September 2013, OECD; Effective Approaches to Support the Implementation of the Remaining G20/OECD High Level Principles on Financial Consumer Protection, September 2014, OECD.

Background

Benefits of digital financial services

The benefits of digital financial services include:

- Extending the potential reach and access of financial services: the digitalisation of finance offers the opportunity to achieve broad-based financial inclusion by extending the availability and penetration of financial services and by reducing the costs of providing financial services to the underserved population.
- Fostering access to financial services for business: new financial technologies can help small and medium-sized enterprises (SMEs), including start-up and scale-up companies, to access alternative funding sources for supporting their cash flow and risk capital needs.
- Offering more convenient, faster, secure and cheaper transactions. This has positive implications in both advanced and emerging economies for businesses and consumers, both established users of financial products and the newly financially included. The latter in particular stand to benefit from a digital environment even in the absence of physical branches or agents, provided appropriate security measures and consumer precautions are in place to avoid fraudulent transactions and other risks.¹²
- Providing services that are tailored to individual needs and facilitate their usage. The use of consumers' data, potentially including big data, by financial services providers can generate insights into individuals' spending habits, facilitating the offer of tailored products and supporting fraud detection. Under the appropriate consumer and data protection framework, these benefits can be substantial for consumers worldwide. They also open up opportunities to integrate the low income and financially excluded populations in the formal financial sector by creating alternative indicators of behaviour that can be used to assess their risk as customers. The digital revolution can also allow consumers to more easily compare offers online and identify the one best suited to their needs.
- Increasing opportunities for fruitful interactions between financial services providers and consumers through digital interfaces. Such interactions can take advantage of behavioural insights, enhancing consumers' understanding of financial products and financial decisions.
- Broadening the range of providers. The digital revolution goes hand-in-hand with new providers entering the market and offering financial services directly to individuals through digital channels can have an impact on the level of competition in the financial market and contribute to lower costs, and offer improved experience to financial consumers.

¹² See for example reports by FinCoNet on *Online and mobile payments: supervisory challenges to mitigate security risks* 2016 and *Online and mobile payments: an overview of supervisory practices to mitigate security risks* 2018.

Box 1. Digital financial services: a definition from the G20/OECD INFE Report

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 well as 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)

Source: OECD (2017), G20/OECD INFE Report on ensuring financial education and consumer protection for all in the digital age www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-Report-Financial-Education-Consumer-Protection-Digital-Age.pdf

Risks of digital financial services

At the same time, digital financial services also carry new risks for financial consumers, in both mature and emerging markets. They can be categorised as follows:

- **Market driven:** this can include misuse of unfamiliar (or new types of) products or to uninformed consumers; new types of fraud, often taking advantage of consumers uncertainty in the digital environment; a lack of security, privacy and confidentiality of data; inappropriate or excessive use of digital profiling to identify potential customers and exclude unwanted groups; rapid access to high-cost/short-term credit or essentially speculative products (e.g. initial coin offerings), and other market practices that can reinforce behavioural biases.
- **Regulation and supervision driven:** this can encompass uneven levels of protection within (e.g. inadequate disclosure and redress mechanisms) and across countries (e.g. variety of providers, cross border selling, regulatory arbitrage); consideration of data protection issues; a lack of coordination among authorities for example with respect to new types of digital financial services.
- **Consumer driven:** the growing digitalisation of daily life and of financial decisions is not necessarily matched by increasing digital and financial literacy levels (OECD, 2016b; OECD, 2017c), and according to OECD studies, this applies even among the younger population (OECD, 2014; OECD 2017b).
- **Technology driven:** the increasing use of algorithms, which can affect decisions about credit, insurance or investments and can lead to denied access to certain services or inappropriate charges based on inaccurate or wrong correlations made without human interpretation; misuse of data including big data and small data (e.g. transactional, airtime data); unreliability of mobile networks and digital finance platforms may lead to inability to carry out transactions, inaccessibility of funds or cybersecurity risks.

These risks can have a negative impact on both consumers and entrepreneurs, and can result in a range of negative outcomes, including, but not limited to:

- Lack of, or uneven, trust and confidence in digital financial services, the financial system and technological innovation.
- New types of exclusion for certain groups of the population (for example the elderly or people on low incomes), lack of comparability or mobility, lack of accuracy or recourse for data correction, due to the increasing use of data and digital profiling for credit, insurance and investment decisions.
- Over-indebtedness among consumers who may be vulnerable.¹³
- Increased customer vulnerability to unfair and deceptive trade practices, including fraud and mis-selling as well as criminal activity such as phishing schemes, account hacking and data theft.

Objectives and Scope

Against this background, this Policy Guidance Note aims to provide a number of updated approaches for financial consumer protection in the digital environment in support of the implementation and application of the DFI and FCP Principles. The updated approaches are designed to provide action-oriented guidance and policy tools and designed to balance the benefits and opportunities of digital financial services, with the potential risks to financial consumers.

In terms of scope, the primary focus of this Policy Guidance Note is on providing guidance relating to:

- Oversight arrangements and capability, i.e. the powers, structures and capabilities of the legal and institutional arrangements required to supervise and enforce financial consumer protection regimes, including responding to changes in business models and service offerings to consumers as a result of digital innovation.
- Disclosure and transparency i.e. developing proportionate service provider requirements for digital financial services relating to disclosure and transparency of the key elements of the product or service, to assist consumer understanding and enforcement of rights.

Focussing on these two areas, as a first step at least, is important in order to establish the foundations of a comprehensive approach to financial consumer protection. These two areas are also the subject of Principle 2 and Principle 4 of the FCP Principles, although many aspects of this Policy Guidance Note are relevant and capable of being applied more broadly. It is anticipated that further guidance will be produced addressing the remaining FCP Principles and as more approaches are developed to protecting the interests of financial consumers.

Given the rapidly evolving nature of the digital environment, and the fact that many new regulatory and supervisory approaches are being tested or trialled, the approaches in this policy guidance should be considered as Innovative or Emerging. They are intended to be flexible, non-binding and designed to

¹³ For example, as a result of immediate credit offers that play on preferences for instant gratification, or high-cost credit with limited checks on affordability.

support jurisdictions to learn from each other and share insights. Further, the approaches are illustrated with examples from the experience to date of individual jurisdictions.

Overarching 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:

- 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.

Oversight arrangements and capability

Technological developments present a range of challenges and opportunities for domestic public authorities responsible for the oversight of financial consumer protection (“oversight bodies”) including inter alia:

- Achieving the right balance between allowing fintech innovations to occur without undue limitations in order to realise the potential benefits for financial consumers, while ensuring an appropriate level of financial consumer protection is maintained. Some oversight bodies have an explicit role to facilitate such innovation in the market, while others do not.
- Ensuring the adequacy of supervisory tools to oversee digital financial services, eg making use of RegTech and/or SupTech (see Box 2) to supplement or enhance their capabilities to supervise the market and monitor risks.
- Ensuring that they have the right mix of resources and capabilities, including capabilities that may not have been traditionally part of a regulator or supervisor’s capability requirements (e.g data analysis), to be able to understand and respond appropriately to new business and distribution models driven by technological innovation.
- Supporting the digital financial literacy of financial consumers to support demand-side capabilities in relation to digital financial products and services.

Box 2. RegTech and SupTech

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:

As part of adapting to an increasingly digitalised environment for financial products and services, oversight bodies around the world are considering the use and application of regulatory technology (“RegTech”). While there is no single definition of RegTech, it can be taken to include:

- use of technology by regulated entities to comply with their regulatory and compliance requirements more effectively and efficiently;
- use of technology by oversight bodies for operations such as market surveillance and risk identification and monitoring (this may be known as “SupTech”).

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 is developing rapidly.^a

RegTech can include the use of artificial intelligence, machine learning and natural language processing, data reporting, regulatory codification and big data analysis technologies.

^a *The Adoption of RegTech within the Financial Services Industry: Ten years from the Start of the ‘Great Financial Crisis’; ESMA, May 2017*

Risks

Policy makers should consider the following innovative and emerging approaches when considering the structures and capabilities of the legal and institutional arrangements required to supervise and enforce financial consumer protection regimes in digital financial services markets, including responding to changes in business models and service offerings to consumers as a result of digital innovation. Practical examples of how these approaches have been applied in different jurisdictions are provided to assist policy makers in their consideration of these approaches.

1. 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.

Jurisdiction approaches

The Bank of **Portugal** launched, in December 2016, 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://cliente bancario.bportugal.pt/sites/default/files/relacionados/publicacoes/QuestCanaisDigitais2016_EN.pdf)

A similar initiative was launched by the Bank of **Italy** in 2017 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-banche-intermediari/Fintech_in_Italia_2017.pdf)

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

Jurisdiction approaches

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 facilitates the exchange of experiences and allows for discussions about new developments in this area. In April 2018, the second edition of the BaFin-Tech will take place in Berlin dealing with topics such as Big Data, Artificial Intelligence, Initial Coin Offerings, Blockchain, Cloud Computing and RegTech.

In November 2017, the Bank of **Portugal** hosted the event "*Paychallenge'17: 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.

Jurisdiction approaches

The **Japan** Financial Services Agency (JFSA) has encouraged financial institutions to enhance their management of cyber-security through monitoring their management system. The supervisory guidelines, published on the JFSA website, provide the viewpoints for the monitoring, as in the following;

- whether the board of directors, etc. recognizes the importance of cyber security amid increasingly sophisticated and cunning cyberattacks and has introduced the necessary control environment
- whether the financial institutions has introduced appropriate cybersecurity management systems as well as setting the organizational structure and rules
- whether the financial institutions has developed contingency plans against potential cyberattacks, conducts exercises (*) and reviews such plans.

(*) JFSA has conducted an annual financial industry-wide exercise (Delta Wall) since 2016, aiming to strengthen cybersecurity in the overall financial sector. In 2017, 100 financial institutions including small and medium sized ones participated in the exercise.

- 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.

Jurisdiction approaches

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.
2. 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.

Jurisdiction approaches

Through the recent 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.

- 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.

Jurisdiction approaches

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.

3. 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.

Jurisdiction approaches

The Central Bank of **Ireland** has set up an internal Fintech Group and, as part of the Central Bank’s regulatory agenda for 2018. This Fintech Group will continue 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.

4. 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.¹⁴

¹⁴ 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.

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.

Jurisdiction approaches

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.

The CSSF in **Luxembourg** has imposed additional disclosure requirements on supervised entities, such as warnings about the specific risks of products or services.

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.

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.

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.

Jurisdiction approaches

In **France**, the French 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.

5. 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.

Jurisdiction approaches

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 17-20. 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.

The Bank of **Italy** has set up, in November 2017, 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. Application from startups and firms that would like 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 of financial services, submitted via a dedicated email address will undergo multifunctional screening that can be tailored to each situation examined in terms of timing and procedures. In the course of the review, operators will be given feedback through meetings and telephone calls, for 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.

At the end of 2015, the Federal Financial Supervisory Authority of **Germany** (BaFin) set up an internal task force which deals with the issues arising through the phenomenon of FinTech and digitalisation. BaFin’s task force is composed of 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 is to keep up with the pace of the newest innovations and to foster regular exchange of information. Another aspect was to check how to smoothen the licensing process for young 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”.

6. 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.

Jurisdiction approaches

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.

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.

One outcome of the task force of the Federal Financial Supervisory Authority of **Germany**, referred to in the example under point 5, is 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>).

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.

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.

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.

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

Jurisdiction approaches

The Bank of **Portugal** has recently introduced changes to the existing regulatory framework to facilitate the opening of bank deposit accounts via digital channels (online e 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/banco-de-portugal-approves-opening-bank-deposit-accounts-video-conference-exclusively).

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.

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.

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.

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).

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.

8. 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.¹⁵

Disclosure and Transparency

Requirements relating to disclosure and transparency in terms of financial products and services are a fundamental part of most financial consumer protection regimes. That said, there is an increasing appreciation of the limitations of disclosure by itself as a consumer protection tool due to people not being able or inclined to read or understand lengthy or complex disclosure documents.¹⁶ Digital developments and the availability of data provide opportunities for policy makers to improve disclosure approaches based on a better understanding of consumer decision-making, and to explore alternatives which may prove more effective. At the same time, new types of disclosure challenges emerge in the digital finance context, associated with such aspects as the use of agents, complex interfaces, limited space in digital devices or opaque terms, conditions and fees, especially regarding complex digital products.

Consideration of disclosure requirements is also relevant to the issue of data privacy in terms of how effectively privacy policies governing the use, collection, sharing and storage of a consumer's personal data are disclosed. (Issues relating to data privacy are of considerable interest to policy makers worldwide, with policy approaches evolving and developing, and are only touched on here in the context of disclosure and possible alternatives.¹⁷)

A number of innovative and emerging approaches are set out below for consideration by policy makers, including practical examples of how these approaches have been applied in different jurisdictions are provided to assist policy makers in their consideration of these approaches.

1. 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.

¹⁵ 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.

¹⁶ See for example: *Addressing financial consumer protection risks in an increasingly digital and financial world A speech by Greg Medcraft, Chairman, Australian Securities and Investments Commission*, OECD-ASIC Asia Pacific Seminar, September 2017.

¹⁷ See for example: *Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy*, Responsible Finance Forum VIII, 27-28 April 2017, Germany.

Jurisdiction approaches

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.

In 2017, the Financial Consumer Agency of **Canada** (FCAC) conducted Public Opinion Research into clear language disclosure in paper-based financial statements.

2. Supporting consumer communications that are clear and simple to understand regardless of the channel of communication.
3. 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).

Jurisdiction approaches

In March 2017, the **Japan** Financial Services Agency published "Principles for Customer-Oriented Business Conduct", comprising 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 935 financial institutions had adopted them as at the end of 2017. The JFSA monitors the implementation of the Principles and will publish KPIs comparable across financial institutions to make their approaches more visible to customers.

4. 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.

Jurisdiction approaches

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; and 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. The study will be finalised by the end of 2018.

5. 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.
6. Testing and exploring new ways of making disclosure more effective for consumers in terms of more targeted, proportionate and customer-centric approaches.

Jurisdiction approaches

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.

7. 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.¹⁸

Jurisdiction approaches

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.

¹⁸ See for example: Mystery Shopping for Digital Financial Services: A Toolkit, Working Paper, CGAP and ITU, April 2017.

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

Jurisdiction approaches

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://cliente bancario.bportugal.pt/pt-pt/noticias/banco-de-portugal-exige-instituicoes-informacao-sobre-os-creditos-que-vao-comercializar>). This also constitutes a way of testing a new oversight tool before new regulatory requirements are issued.

8. 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.
9. 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.
10. 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.

Jurisdiction approaches

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.^a 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. Specific guidance on consent will be provided by national data protection authorities. The GDPR also includes provisions relating to privacy by design.

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.^b

^a General Data Protection Regulation (EU) 2016/679

^b The Appropriate Use of Customer Data, World Economic Forum, December 2017

REFERENCES

- Consumers International (2017), Banking on the Future: An exploration of fintech and the consumer interest www.consumersinternational.org/media/154710/banking-on-the-future-full-report.pdf
- FinCoNet (2017), Report on the Digitalisation of Short-Term, High Cost Consumer Credit www.finconet.org/Digitalisation-Short-term-High-cost-Consumer-Credit.pdf
- G20 (2016), G20 High-Level Principles for Digital Financial Inclusion. www.gpfi.org/sites/default/files/G20%20High%20Level%20Principles%20for%20Digital%20Financial%20Inclusion.pdf
- G20 (2010), G20 Principles for Innovative Financial Inclusion. www.gpfi.org/sites/default/files/documents/G20%20Principles%20for%20Innovative%20Financial%20Inclusion%20-%20AFI%20brochure.pdf
- G20/OECD (2011), High-level Principles on Financial Consumer Protection. www.oecd.org/daf/fin/financial-markets/48892010.pdf
- GSMA (2016b), 2015 State of the Industry Report Mobile Money, Groupe Speciale Mobile Association, London. www.gsma.com/mobilefordevelopment/wp-content/uploads/2016/04/SOTIR_2015.pdf
- OECD (2015), OECD Digital Economy Outlook 2015 <http://dx.doi.org/10.1787/9789264232440-en>
- OECD (2017), G20/OECD INFE Report on ensuring financial education and consumer protection for all in the digital age www.oecd.org/daf/fin/financial-education/G20-OECD-INFE-Report-Financial-Education-Consumer-Protection-Digital-Age.pdf
- OECD (2017), Technology and innovation in the insurance sector <https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf>
- Insurance Association of Insurance Supervisors (2017), Fintech Developments in the Insurance Industry www.iaisweb.org/file/65625/report-on-fintech-developments-in-the-insurance-industry
- Responsible Finance Forum (2017), Opportunities and Risks in Digital Financial Services: Protecting Consumer Data and Privacy <https://responsiblefinanceforum.org/publications/key-takeaways-eighth-responsible-finance-forum/>
- Responsible Finance Forum (2018), Investor Guidelines: Investing in Responsible Digital Inclusion <https://responsiblefinanceforum.org/investor-guidelines/>
- World Bank Group (2017), Global Financial Inclusion and Consumer Protection Survey, 2017 Report <https://openknowledge.worldbank.org/bitstream/handle/10986/28998/122058.pdf?sequence=2&isAllowed=y>
- World Economic Forum (2017), Briefing Document, The Appropriate Use of Customer Data <https://weforum.ent.box.com/s/z3op26ib9ttfr3b28zzccu0bftzx6br1>

ABOUT THE “G20/OECD POLICY GUIDANCE ON FINANCIAL CONSUMER PROTECTION IN THE DIGITAL AGE”

This policy guidance is for consideration by policy makers responsible for the implementation and application of key elements of the G20/OECD High-Level Principles on Financial Consumer Protection in a digital environment and G20 High-level Principles on Digital Financial Inclusion with respect to principle 5. It focuses on areas related to the role of oversight bodies and disclosure and transparency. It has been developed by the G20/OECD Task Force on Financial Consumer Protection.

This policy guidance is complemented by a Policy Guidance note on Digitalisation and Financial Literacy, developed through the OECD/International Network on Financial Education (INFE), which addresses the implementation of Principle 6 of the G20 High Level Principles for Digital Financial Inclusion.

ABOUT THE G20/OECD TASK FORCE ON FINANCIAL CONSUMER PROTECTION

The Task Force was established in 2010 in response to the financial crisis and in recognition of the fact that appropriate financial consumer protection – together with access to appropriate financial products and good quality financial education – are fundamental requirements for consumer trust and confidence in the market.

The Task Force is responsible for the Financial Consumer Protection Principles, first endorsed by the G20 in 2011. The Principles are designed to assist policy makers in developing comprehensive financial consumer protection frameworks. They are widely acknowledged and their implementation is monitored by the Task Force on an ongoing basis.

www.oecd.org/finance/financialconsumerprotection.htm

✉ daf.contact@oecd.org

FOR MORE INFORMATION, PLEASE CONTACT:

Ms. [Flore-Anne Messy](#), Head of the Financial Affairs Division, OECD
and Executive Secretary of the OECD/INFE

✉ Flore-Anne.MESSY@oecd.org

www.oecd.org/finance



This report contributes to the OECD Going Digital project which provides policy makers with tools to help economies and societies prosper in an increasingly digital and data-driven world. For more information, visit www.oecd.org/going-digital.

