Financial Consumer Protection Policy Approaches in the Digital Age

Protecting consumers' assets, data and privacy

Please cite this publication as:

OECD (2020), *Financial Consumer Protection Policy Approaches in the Digital Age: Protecting consumers' assets, data and privacy.*www.oecd.org/finance/Financial-Consumer-Protection-Policy-Approaches-in-the-Digital-Age.pdf

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, as well as any data and 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, now further accelerated by responses to the COVID-19 pandemic, and the potential for digitalisation to support greater financial inclusion and inclusive growth, 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 evolve and adapt in line with the changing environment.

Digitalisation can bring many benefits to financial consumers, but also comes with new risks. Positive outcomes include greater access to, and choice of, products and services available for consumers at lower costs, expanded speed, convenience, personalisation and security. Risks include new forms of theft or fraud perpetrated online, data breaches, lack of privacy and digital security incidents.

This policy guidance note has been developed under the programme of work of the G20/OECD Task Force on Financial Consumer Protection. It is the latest guidance designed to support the implementation of the G20/OECD High Level Principles on Financial Consumer Protection in the digital environment. It sets out flexible and non-binding guidance for policy makers and oversight authorities relating specifically to Protection of Consumer Assets against Fraud and Misuse and Protection of Consumer Data and Privacy. Jurisdiction specific examples illustrating the application of the guidance can be found in the Compendium of Effective Approaches.

Acknowledgements

This Policy Guidance Note has been produced by Miles Larbey, Head of Financial Consumer Protection at the OECD, working closely with an Expert Group of Task Force delegates and with support from Flore-Anne Messy, Head of the Insurance, Private Pensions and Financial Markets Division, OECD. It has been developed via an extensive consultative and iterative approach, based on inputs, comments and feedback from members of the Task Force, as well as other relevant OECD networks and committees including the Working Party on Security in the Digital Economy, the Working Party on Digital Governance & Privacy and the Consumer Policy Committee. We would like to acknowledge and thank all delegates for their participation and contribution to the development of the guidance

Table of Contents

Boxes

Introduction

Digitalisation in the form of technological innovation is having an ongoing transformative impact on societies and economies. In relation to financial services, digitalisation has significantly affected all sectors ranging from payments to banking and saving to insurance to investing, with the emergence of many new products, services, distribution models by existing market players and new entrants such as tech companies both large and small.

On the supply side, the explosion in the generation and use of data combined with significantly enhanced computing power, processing and analytical capabilities using data analytics and machine learning (artificial intelligence) has allowed financial services providers to continuously innovate to better serve their customers and enhance their profitability.

On the demand side, the appetite among consumers for easy to access, simple, attractive and low cost digital financial services has grown thanks to increased internet and smartphone penetration and interoperability, and is only expected to continue to increase as the digitally aware and savvy population cohorts such as Gen Z join the labour and financial markets.

The benefits of digitalisation for financial consumers are significant: fintech innovations provide financial consumers with wider choice at lower costs, expanded speed, convenience, personalisation and security. They have the potential to support greater access to financial products and services thereby supporting financial inclusion. Digitalisation also acts as a spur for competition by expanding the range of providers via new entrants, contributing to increasing efficiency of operations of financial services providers and facilitating comparison shopping and switching of products.

There are also new risks to consumers associated with digitalisation specific to the financial services sector which need to be monitored and addressed. Such risks include new forms of theft or fraud perpetrated online, data breaches and digital security incidents, excessive data profiling leading to financial exclusion, lack of privacy and manipulation of consumers' behavioural biases when operating online. Moreover, the nature of digital security risk is extremely dynamic, with the continuous appearance of new threats and identification of new vulnerabilities.

In this increasingly digital environment and faced with these new and evolving risks, the need for effective financial consumer protection, including data protection, is more important than ever. The policies and approaches developed and adopted by financial consumer protection policy makers and oversight bodies need to evolve and adapt in line with the digital environment.

This Policy Guidance Note is the latest in a series of guidance notes designed to support the implementation of the G20/OECD High Level Principles on Financial Consumer Protection ("the FCP Principles") in the digital environment. It sets out flexible and non-binding guidance for policy makers and oversight authorities relating specifically to two of the ten FCP Principles, namely:

a. Protection of Consumer Assets against Fraud and Misuse (Principle 7)
b. Protection of Consumer Data and Privacy (Principle 8).

The guidance is based on the input of members of the G20/OECD Task Force on Financial Consumer Protection and reflects many of the practices and approaches that are being adopted or trialled in different jurisdictions. In this way, the guidance is designed to support jurisdictions to learn from each other and share insights. Recognising the importance of data protection as part of the overall approach to protecting financial consumers in the digital environment, the guidance also draws on the expertise and inputs of data protection policy makers and regulators.

Background and Policy context

Financial Consumer Protection

Financial consumer protection refers to the framework of laws, regulations and other approaches generally designed to ensure fair and responsible treatment of financial consumers in their purchase and use of financial products and their dealings with financial services providers.

Established in response to the financial crisis of 2008, the G20/OECD Task Force on Financial Consumer Protection ("the Task Force") is the leading global forum for the development of financial consumer protection policy and practice internationally. The Task Force is responsible for the *G20/OECD High-Level Principles on Financial Consumer Protection* ("the FCP Principles"), which were issued in 2011 and 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.

The Principles cover the following areas:

Legal, Regulatory and Supervisory Framework	Responsible Business Conduct of Financial Services Providers and Authorised Agents
Role of Oversight Bodies	Protection of Consumer Assets against Fraud and Misuse
Equitable and Fair Treatment of Consumers	Protection of Consumer Data and Privacy
Disclosure and Transparency	Complaints Handling and Redress
Financial Education and Awareness	Competition

The Principles are supported by non-binding, practical and evidence-based guidance 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.

The financial services sector is dynamic, characterised by constant changes as a result of market, technological and legal developments. Whereas the Principles are intended to be evergreen as far as possible, therefore, the Effective Approaches are designed to be kept up to date in line with changes in the environment.

In light of this, a key workstream of the Task Force is to update the Effective Approaches to reflect the ever greater digitalisation of financial products and services. The updates consider the implications of digitalisation for financial consumer protection policy and the regulatory challenges and opportunities arising from financial innovation. Work conducted to date is as follows:

2018	Development of updated effective approaches to support the implementation of FCP Principles 2 (Role of Oversight Bodies) and Principle 4 (Disclosure and Transparency) - this work formed the basis of the 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.
2019	Development of updated effective approaches to support the implementation of FCP Principles 1: Legal, Regulatory and Supervisory Framework; 3: Equitable and Fair Treatment of Customers; 6: Responsible Business Conduct; 9: Complaints Handling and Redress - the updated effective approaches are set out in the consolidated Effective Approaches for Financial Consumer Protection.

In 2020, the Task Force undertook to develop updated Effective Approaches for the following Principles:

- Principle 7: Protection of Consumer Assets against Fraud and Misuse, which relates to such matters as protection of consumer assets against frauds and scams, misappropriation and misuse
- Principle 8: Protection of Consumer Data and Privacy, which relates to such matters as collection, use and storage of personal data by financial services providers, credit reporting systems and data sharing.

Digitalisation developments have had a major impact on the implementation of both Principle 7 and 8 since they were first issued in 2011. This Policy Guidance Note discusses relevant developments and issues in Chapter 1 and then sets out updated effective approaches in Chapter 2.

Data Protection and Privacy

Data protection and privacy are important and developing policy areas that extend across all sectors of the economy.

The OECD first developed the *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* in 1980. The Guidelines were comprehensively revised and updated in 2013 in view of the structural changes in the societal and technological environment in which they operate. As noted in review work, today’s economies present substantial differences in:

- the volume of personal data being collected, used and stored
- the range of analytics involving personal data, providing insights into individual and group trends, movements, interests, and activities
- the value of the societal and economic benefits enabled by new technologies and responsible uses of personal data
- the extent of threats to privacy
- the number and variety of actors capable of either putting privacy at risk or protecting privacy
- the frequency and complexity of interactions involving personal data that individuals are expected to understand and negotiate
- the global availability of personal data, supported by communications networks and platforms that permit continuous, multipoint data flows.

In line with the significant developments in the generation and use of data, there have been significant developments in many jurisdictions regarding the regulation of data protection and/or privacy. For example, in the European Union, the *General Data Protection Regulation* (GDPR) became effective in May 2018 and aims to give more controls to EU citizens over their personal data, and how they are accessed, processed and used. In South Africa, the *Protection of Personal Information Act 2013* came into effect in 2020 and sets out eight conditions for lawful data processing. In Japan, the *Act on the Protection of Personal Information* was first adopted in 2003, and has been substantially amended in 2015 and again in 2020.

In a number of jurisdictions, the laws and regulations relating to data protection and/or privacy are administered and enforced by dedicated data protection authorities. Such authorities are generally responsible for data protection across the economy and not in relation to specific sectors. In other jurisdictions, there are sector-specific privacy laws for consumer financial services that are enforced by consumer protection and other regulators.

In terms of the nexus between financial consumer protection and data protection, while financial consumer protection regulators and supervisors do not generally have primary responsibility for administering general privacy or data protection laws, they generally have a role to play insofar as they may constitute breaches of sector-specific financial privacy laws or when breaches of personal data protection laws are associated with breaches of financial consumer protection laws. Furthermore, financial services providers increasingly use data in the design and distribution of financial products and services to consumers, the marketing and conduct of which falls under the scope of financial consumer protection regulators and supervisors.

Financial Education

While the focus of this Policy Guidance Note is on the supply side, measures to support the demand side form an important part of the overall policy context in this space.

The OECD/International Network on Financial Education has established a Working Group to strengthen financial literacy and awareness on issues around personal data. In 2020, the Working Group published a report on *Personal Data Use in Financial Services and the Role of Financial Education: A Consumer Centric Analysis,* which among other things sets out new elements to address the use of personal data within financial education programmes and to encourage positive behaviours on personal data awareness and management.

This Policy Guidance Note can be seen as complementary to the report on financial education.

Process

This Policy Guidance Note was developed under the aegis of the Task Force as part of the overall process to update the Effective Approaches that support the FCP Principles. The guidance reflects inputs and feedback from Task Force members.

Given the subject matter of the particular Principles under review and the differing legal and regulatory responsibilities relating to data protection, the guidance was developed in consultation with data and consumer protection policy makers and authorities to ensure that their expertise was fully incorporated.

To that end, in addition to consultation by Task Force members with their regulatory counterparts at a bilateral level, the Task Force Secretariat also sought input and comments from relevant OECD networks and committees, including:

- Working Party on Security in the Digital Economy
- Working Party on Digital Governance & Privacy
- Consumer Policy Committee.

This Policy Guidance Note therefore incorporates comments and feedback received from a wide range of relevant stakeholders via a comprehensive iterative and consultative process.

Digitalisation in the financial services industry

Digitalisation is transforming the financial services industry and the way that consumers interact with financial products and service providers, driven by rapidly expanding mobile technologies, enhanced data processing and analytical capabilities and increased connectivity between smart devices and financial services platforms and applications.

To illustrate this expansion, in 2005, around 56% of the adult population in OECD economies accessed the Internet, and 30% used it daily. In 2016, these percentages rose to 83% and 73%, respectively.[1] According to GSMA's State of the Industry Report on Mobile Money, 2019 saw the number of registered mobile money accounts globally surpass one billion for the first time and the number of digital transactions exceed cash-based transactions.[2]

Digitalisation affects all parts of the financial services industry, with technological driven innovations occurring in payments (instant payment, digital wallets) to credit (crowdfunding and online market lending), insurance (insuretech) and investment (robo-advice) to core banking (online digital banks), biometric identification or back-end support services (cloud-computing and big data).

Benefits and Risks

The benefits and risks of increased digitalisation for consumers of financial services are set out in detail in *Financial Consumer Protection Approaches in the Digital Age.* In summary, benefits for consumers include:

- Extending the reach and access of financial services thereby supporting broad-based financial inclusion
- Fostering access to financial services for businesses, including start-ups and scale-up companies
- More convenient, faster, secure and cheaper transactions
- More individually tailored financial products and services
- Increased opportunities for fruitful interactions between financial services providers and consumers through digital interfaces
- Broadening the range of providers of financial services to include new entrants such as fintechs as well as incumbent market players.

Risks to consumers may be categorised as:

- Market driven risks, including misuse of unfamiliar products, new types of fraud, lack of security, increased speed of transactions leading to greater likelihood of violation of consumer rights (e.g.,

[1] OECD (2017), Technology and innovation in the insurance sector

[2] GSMA (2019), State of the Industry Report on Mobile Money 2019

right to clear information, right to be protected from misleading or false advertising), lack of privacy and confidentiality, excessive use of digital profiling leading to financial exclusion;

- Regulation and supervision driven risks, such as uneven level of protection within or across jurisdictions, non-compliance with obligations of financial services providers to meet general conditions for negotiation and pre-formulated contracts;
- Consumer driven risks, such as low levels of digital or financial literacy contributing to financial exclusion particularly among vulnerable consumers, the impact of digital transactions on behavioural biases;
- Technology driven risks, such as increased use of algorithms and the outcomes generated, issues relating to access or reliability of digital networks; cybersecurity risks.

Digitalisation driven developments and innovations

Digitalisation is transforming how consumers interact with financial products and services. Some of the key developments and innovations include:

- *Mobile and online banking*: there has been a rapid uptake in the use of mobile and online banking among consumers, which for many represent greater convenience and security. For example, according to data gathered across 20 countries by GlobalData, on average, 42% of online consumers with a current account used mobile banking on a daily or weekly basis in 2018, up from 39% in 2017.[3] At the same time, bank branches are in decline
  - A related development is the emergence of *digital banks*, which exist solely online with no physical locations, doing away with the need for a branch network altogether.
- *New entrants and applications:* the digital environment for financial services has been characterised by new entrants, with many fintechs offering digitally disruptive products and services in competition to or in partnership with existing market players. As well as many small players, new entrants include BigTech companies, such as Apple, Google, Facebook etc. Both new entrants and existing players offer an ever-increasing range of new mobile applications and tools [4] ranging from budgeting or spending tracking apps, customer service applications such as chatbots to account aggregation services or open APIs involving third parties. Open Banking regimes, which have been introduced or are under consideration in a number of jurisdictions, facilitate the exchange of data among banks or between banks and fintechs and other third parties. One of the objectives of Open Banking is to foster competition and innovation, which may result in new entrants and applications.
- *Digital or mobile payments and digital wallets*: these services are transforming the way that payments are made by consumers. Mobile payments using near-field communication technology allow consumers to make payments by waving their smartphone across a reader, with an estimated 1 billion people predicted to use a mobile payment application in 2020.[5] Global market leaders include Alipay, WeChat, Apple Pay and PayPal. Digital wallets allow users to send, receive and store money electronically. According to a report by RetailDive, around 2.1 billion people used digital wallets in 2019, which was an increase of 36% over 2018.[6]

[3] https://www.globaldata.com/global-mobile-banking-usage-highest-india-sweden-sees-fastest-growth-says-globaldata/

[4] https://digitalmarketinginstitute.com/blog/how-is-digital-changing-the-financial-industry

[5] https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/#global

[6] https://www.retaildive.com/news/21b-consumers-will-use-mobile-payments-by-2019/520652/

- *Automated risk assessment and decision-making*: financial services providers increasingly use digitalisation in the process of risk assessment and associated decision-making in particular relating to credit and insurance.
  - In relation to credit, artificial intelligence in the form of predictive analytics can make use of thousands of data points, including alternative data, to inform individual credit scoring and creditworthiness assessments.
  - In relation to insurance, data aggregation may be used to achieve more precise risk segmentation and risk-based pricing.[7] For example, data analytics can be applied to telematics data that monitors the behaviour of policyholders and used to mitigate risk in advance and determine pricing, for example in relation to motor or health insurance. Online interfaces and virtual claims adjusters can also make it more efficient to settle and pay claims following an accident.
- *Robo or digital advice*: this is a term used to describe digital platforms which offer automated wealth management and advisory services using algorithms to support the decision-making. Consumer data is processed to understand clients' needs, time horizon and assess risk tolerance and generate recommendations. Robo advice platforms have the potential to increase the accessibility of investment advice and reduce costs. Such platforms are being developed by existing market players and new entrants, with an estimated USD 1 trillion assets under management in 2020.[8]
- *Fraud detection*: increasingly, banks and credit providers are using machine learning and artificial intelligence to help identify potential fraud in milliseconds thanks to near-time (i.e. almost instantaneous) monitoring and continuous analysis of spending and account management patterns. Such fraud detection and prevention may be used in relation to identify theft, credit card fraud and insurance fraud.
- *Cryptocurrencies or cryptoassets*. Cryptoassets, in the form of digital or cryptocurrencies and initial coin offerings (ICOs) have recently captured the interest of the public and policy makers around the world. Starting most notably with Bitcoin, and enabled by blockchain technologies, a proliferation of cryptoassets has become available which, regardless of their stated purposes, have been attractive to some as investment opportunities, fuelled in some cases by significant price increases or the perceived potential for such.

Data processing and analytics

The developments and innovations outlined above are all underpinned by the explosion in recent times in the generation, collection, storage, sharing and use of personal and transactional data. According to a report by International Digital Corporation, the growth in digital data created will grow from 33 Zettabytes (ZB) in 2018 to 175 ZB in 2025. To help give this some context, the total amount of information in existence in 2011 was around 1.2 ZB.[9] The same report predicts that by 2025, each connected person will have at least one data interaction every 18 seconds.[10]

This explosion in data is generated from activities carried out electronically and from machine-to-machine communications enabled by such advances in digital technology, such as smart devices, connected devices and greater interoperability,]Internet of Things (IoT) and advances in biometrics. The generation

[7] OECD (2017), Technology and innovation in the insurance sector

[8] OECD (2017), Robo-Advice for Pensions

[9] OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being

[10] The Digitization of the World: From Edge to Core: An IDC White Paper, IDC, November 2018

of these huge amounts of data, at levels unprecedented in human history, is referred to as "big data". Big data have characteristics summarised as "3V" (volume, variety and velocity):

- Volume, referring to vast amounts of data generated over time;
- Variety, referring to the different formats of complex data, either structured or unstructured (e.g. text, video, images, voice, documents, sensor data, activity logs, click streams, co-ordinates, etc.);
- Velocity, referring to the high speed at which data are generated, become available and change over time.[11]

Data is being increasingly generated and used across all industries, with data intensity highest in the financial services sector (including securities and investment services and banking). There is a wide range of internal and external sources of Big Data available to financial services providers, such as:

- CRM information, product-related information, security information held by the provider
- IoT sensor data such as car telematics, wearables, home sensors, geolocation data
- Unstructured data relating to communications with customers such as emails, chat sessions, voice and video recordings, call logs etc.
- Customer behaviour on websites such as browsing patters
- Data gathered from APIs involving third parties (eg open banking applications)
- Social media data.[12]

Financial services providers are able to create business value from these sources of data because of significantly enhanced data processing and analytical capabilities, which allow them to use data to drive growth, better target, serve and retain serve customers through more personalised marketing and products and service offerings, reduce costs and enhance their risk management and regulatory compliance.

Techniques and tools used by financial services providers to extract information and create patterns from data are referred to as analytics (or "predictive analytics") refers to a set of. Advances are most notable, and have the most important consequences in the financial services industry, in the following areas:

- *Data mining*: the set of techniques used to extract information patterns from data sets.
- *Profiling*: the use of data analytics for the construction of profiles and the classification of individual consumers in specific profiles. Credit scoring, price discrimination and targeted advertisements are typical examples of activities involving profiling.
- *Machine or statistical learning* is a subfield in computer science, and more specifically in artificial intelligence. It is concerned with the design, development and use of algorithms3 that allow computers to "learn" – that is, to perform certain tasks while improving performance with every empirical data set they analyse. Machine learning involves activities such as pattern classification, cluster analysis, and regression. Due to the high volume of financial data generated, machine learning has found many applications across the financial services sector.[13]

[11] OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being

[12] Big Data in the Financial Services Industry – from data to insights, J Lochy, Finextra, September 2019

[13] OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being

Box 1. Artificial Intelligence (AI)

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.

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 with Argentina, Brazil, Malta, Peru, Romania and Ukraine having adhered to the Principles thus far.

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.

In June 2019, the G20 adopted human-centred AI Principles that draw from the OECD AI Principles.

Source: OECD (2019) Recommendation of the OECD Council on Artificial Intelligence

Protection of Consumer Assets

Protection of consumer assets is concerned with the protection of consumers' financial assets, such as deposits, from fraud, misappropriation and misuse. It is a fundamental part of an overall financial consumer protection framework and includes arrangements covering fraudulent or unauthorised payments, segregation of customer assets and procedures for protecting and recovering unclaimed assets.

In the digital environment and given the ever-increasing range of digital applications and tools available to consumers, the protection of consumer assets extends to encompass to protecting consumers' data from the risk of digital security incidents, including cyberattacks, systems failures or data breaches at financial institutions, as well as online scams and frauds targeted financial consumers directly.

Digital security

Digital security is an increasingly important issue for all governments and industry sectors as the likelihood and severity of digital security incidents has grown in recent years. The financial services sector is attractive to digital security incidents due to the potential value of the data and information stored by financial services providers. The sector is further exposed through such things as outsourcing of internal processes, shift to cloud computing and connecting with customers through more channels, all of which enlarges the "attack surface".[14]

Financial services providers are investing significant amounts of resources on the adoption of security measures to avoid data loss, corruption, destruction, unauthorised access, manipulation or misuse of such data. Notwithstanding, the likelihood and severity of digital security incidents continues to rise. In the United Kingdom alone, for example, financial services providers reported a total of 819 digital security incidents to the UK Financial Conduct Authority in 2018, out of which 93 were classified as cyber-attacks, 174 occurred due to third-party failure, and 157 occurred due to hardware or software issues.[15]

Box 2. Digital security incidents in financial services

Digital security incidents affecting the data stored by financial services providers have become more common and more serious in line with the exponential growth in the collection and use of data. The examples below illustrate the significance of such incidents in the financial services sector:

- In July 2019, Capital One announced that it had suffered a data breach compromising the credit card applications of around 100 million individuals after a software engineer hacked into a cloud-based server. The applications contained names, dates of birth, credit scores, contact information, and some US and Canadian social security numbers.
- In October 2017, the credit reporting agency Equifax announced that more than 150 million customer records had been compromised by hackers, including some sensitive data such as birth dates and 12,000 US social security numbers.
- In November 2016, Tesco Bank, a retail bank based in the UK, was the target of thieves who used vulnerabilities in its card issuing process to guess bank card numbers and steal £2.26 million in November 2016. The unknown attackers likely used an algorithm to generate bank card numbers that used Tesco's identifying numbers at the start and conformed to the industry-wide Luhn validation scheme that helps protect against accidental errors. Tesco Bank halted all online and contactless transactions after a day of struggling to block all the fake purchases reported in the United States, Spain, and Brazil.

Source: Carnegie Endowment for International Peace, Timeline of Cyber Incidents involving Financial Institutions, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

Online frauds and scams

As well as digital security incidents targeting the data and systems of financial services providers, consumers themselves are also targeted by a wide range of online frauds and scams. Such activity has increased in line with the growth in digital transactions. While it is impossible to know the full extent of

[14] PwC Financial Services, *Top financial services issues of 2018,* December 2017

[15] https://www.teiss.co.uk/financial-firms-cyber-incidents-fca/

online frauds and scams targeting consumers due to underreporting, according to the 2019 Data Book of the Consumer Sentinel Network operated by the Federal Trade Commission in the USA, 3.2 million reports of fraud and identify theft were received by the network. Of the 1.7 million fraud reports, 23% indicated money was lost. In 2019, people reported losing more than $1.9 billion to fraud – an increase of $293 million over what was reported in 2018.[16]

Common types of online frauds and scams targeting financial consumers include:

- *Advance fee frauds*: these frauds have various different forms but they all involve an email or other communication inviting the victim to pay money in return for receiving something of greater value such as a prize, inheritance, investment or transferred money. Advanced fee frauds include Nigerian scams, lottery scams, unexpected inheritance scams, dating and romance scams
- *Bank loan or credit card scams*: these scams take the form of fraudulent bank loan offers in return for victims' sending their personal details, stealing and unauthorised use of credit cards or "skimming" credit card information.

Online frauds and scams are also commonly committed through digital security attacks using the following techniques:

- *Phishing and social engineering:* the attacker attempts to use communications such as emails or social networks to trick consumers into providing valuable personal data such as passwords, log-in details or bank account details. Often the communications appear to come from an official source and invite victims to click on a link and enter their details via a fraudulent website.
- *Malware attacks*: victims click on a link or attachment that installs or executes malicious software on their computer allowing the perpetrator to steal personal details and commit fraudulent activities such as unauthorised transactions. Ransomware is a type of malware that blocks or limits access to a computer or file with a demand for a ransom be paid to the scammer for them to be unlocked.

Efforts by consumer protection authorities to tackle online frauds and scams are particularly challenging because the perpetrators are not authorised or licensed and may not even be based in the jurisdiction. On the other hand, and as noted above, increasingly, banks and credit providers are using digitalisation in the form of machine learning and artificial intelligence to help identify potential fraudulent activity.

New types of fraudulent or unauthorised payments

As noted above, digitalisation is transforming the way that payments are made by consumers, with innovations such as contactless payments, digital wallets, smart phone or smart speaker payments being increasingly taken up by consumers. Innovations in new types of payment also increases the scope for fraudulent or unauthorised payments. According to the OECD Recommendation on Consumer Protection in E-Commerce, businesses should, inter alia, implement security measures that are commensurate with payment-related risks, including those resulting from unauthorised access or use of personal data, fraud and identify theft.[17] An example of a new type of fraudulent payment arising from greater use of digital payments is "authorised push payment fraud". Authorised push payments are payments made when consumers tell their financial institution to make a payment from their account to another account. Scams involving authorised push payments occur when consumers are tricked into authorising a transfer of money to an account that they believe belongs to a legitimate payee but is in fact controlled by a scammer.

[16] Consumer Sentinel Network Data Book 2019, Federal Trade Commission, January 2020

[17] OECD (2016), Consumer Protection in E-commerce: OECD Recommendation

Protection of Consumer and Data Privacy

As noted above, there is a clear nexus between financial consumer protection and data protection and privacy. Also as noted, there have been significant developments in terms of laws and regulations relating to data protection and privacy, applicable across all sectors of the economy.

Given the prevalence and intensity of data generation and use in the financial services industry, this Policy Guidance Note addresses the implications of the use of data in the financial services industry and the risks that are specific to financial products and services.

A particular focus has been on the use data analytics in the form of machine learning algorithms in the process of risk assessment and associated decision-making in particular relating to credit and insurance. While this has many benefits as outline above, this trend also creates risks of unintended or undesirable consequences such as bias or errors, which may in turn contribute to inadvertent discrimination and financial exclusion. For example, in insurance, while the use of data analytics may increase precision in the pricing of individual insurance policies, it also may push the boundaries of the goal of insurance to pool risks and lead to exclusion from insurance for risks deemed to be "bad risks".[18] There are also potential consequences for consumers who choose to opt out of data sharing, such as risks of being excluded or receiving less advantageous pricing (known as the 'privacy premium').

This raises a number of considerations for policy makers, regulators and supervisors as they seek to regulate such services in particular relating to such matters as transparency, accountability and fairness in terms of outcomes generated by the algorithms. Related to this is the idea of explainability, i.e. attempts to explain and thereby understand the decisions arrived at via use of algorithms.[19]

Another issue that arises is in the context of consumer and data privacy is that of consent. Generally speaking, informed consent provides the main legal basis for the collection and processing of data. As noted below, research conducted for the UK Financial Consumer Panel found that in many cases consumer consent was not well informed with most people either not reading terms and conditions or privacy notices or not understanding them if they did.[20] It is important that requests for consent are as clear and understandable as possible avoiding the use of language or terminology of an excessively legal, technical or specialised nature. In addition, the *G20 Policy Guide on Digitisation and Informality* published in 2018, sets out a number of possible ways of enhancing informed consent such as tiered consent models, expiry dates for consent, opt-in rather than opt-out consent and recording of consent by industry participants.[21]

[18] OECD (2018), Financial Markets, Insurance and Private Pensions: Digitalisation and Finance

[19] https://www.fca.org.uk/insight/explaining-why-computer-says-no

[20] https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf

[21] https://www.gpfi.org/sites/gpfi/files/documents/G20_Policy_Guide_Digitisation_and_Informality.pdf

Box 3. Consumer attitudes towards privacy and data as a commodity

As well as regulatory and technology issues, consumers' attitudes and behaviours towards privacy and data as a commodity are relevant to consideration of data protection. As noted in the OECD report *A consumer-centric analysis of personal data use in financial services and the role of financial education,* the response of consumers to developments and to the opportunities and risks offered by big data are mixed. The report identifies the following issues relating to consumer attitudes:

- *Data privacy concerns*: evidence suggests consumers value their privacy and are aware of how this can be compromised in today's technological environments. For example, a 2019 ICGI-Ipsos Global Survey on Internet Security and Trust showed that over half of internet users surveyed globally were more concerned about their online privacy than they were in the previous year.22 At the same time, not all consumers apply the necessary steps to safeguard their personal data online.
- *Trading personal data for additional benefits*: evidence suggests that consumers are willing to share additional personal data with financial providers if this results in perceived benefits. For example, according to a survey conducted by Accenture in 2019, around 60% of the consumers surveyed globally indicated that they would share more data with banks, insurers or investment advisory firms if this translated into priority services, pricing benefits, more personalised products or non-regulated financial advice.
- *Consent is not well informed*: evidence suggests that when it comes to sharing data, consumer consent is not well informed. For example, research conducted by the Financial Services Consumer Panel in the UK in 2018 found that more than three quarters of consumers state that they do not feel informed when they read terms and conditions.23

Source: OECD (2020) Personal data use in financial services and the role of financial education

Given the limitations of consent based models, a range of alternative and complementary approaches are being increasingly adopted as part of data protection frameworks. One such approach is "privacy by design" whereby technologies, processes, and practices to protect privacy are built into system architectures, rather than added on later as an afterthought.[24]

Another approach is that of "data minimisation". As set out in the G20 Policy Guide on Digitisation referred to above, this approach involves identifying data items that are relevant for risk evaluation, identifying those data items that should only be captured and used under specific circumstances or allowing industry participants to evidence the relevancy of such data to the purpose of risk evaluation. This approach envisions that only the minimal amount of data should be collected.[25]

A complementary approach involves requiring data collectors and data processors to demonstrate a "legitimate interest" in processing a particular type of personal data. For example, the EU's GDPR incorporates this concept through the six available bases for processing personal data: consent; contract; legal obligation; vital interest; public task; and legitimate interests. India's draft Personal Data Protection

[22] https://www.cigionline.org/internet-survey-2019

[23] https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf

[24] https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

[25] https://www.gpfi.org/sites/gpfi/files/documents/G20_Policy_Guide_Digitisation_and_Informality.pdf

Bill includes equivalent requirements pertaining to legitimate purposes for data processing as well as obligations for “data fiduciaries”.

Financial Consumer Protection in the Digital Age: Effective Approaches

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. 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, consumer protection and non-financial sectors such as telecommunications, to promote consistency where appropriate.

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.

The policy guidance below sets out practical, non-binding policy guidance to support the implementation of Principle 7 in the digital environment.

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)

In particular, the following provisions of the OECD Recommendation on Consumer Protection in E-Commerce (2016) relating to e-payments are relevant:

- Businesses should provide consumers with easy-to-use payment mechanisms and implement security measures that are commensurate with payment-related risks, including those resulting from unauthorised access or use of personal data, fraud and identity theft .

Effective Approaches to support the implementation of Principle 7

a. 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.

b. 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).

c. 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.

d. 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.

e. 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.

f. 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").

g. 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.

h. 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).

i. 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.

j. 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.

k. 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.

l. 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. [26]

m. 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.[27] 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.

n. 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.

o. 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.

p. 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.

q. 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.

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

[27] Ibid

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 also relevant and should be taken into account:

- 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)

In particular, the OECD Recommendation on Consumer Protection in E-Commerce makes clear that businesses should protect consumer privacy by ensuring that their practices relating to the collection and use of consumer data are lawful, transparent and fair, enable consumer participation and choice, and provide reasonable security safeguards.[28]

Effective Approaches to support the implementation of Principle 8

The policy guidance below sets out practical, non-binding policy guidance to support the implementation of Principles 8 in the digital environment.

a. 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.

b. 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 decision about their data at a relevant time and context.

c. 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.

d. 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.

[28] OECD (2016), Consumer Protection in E-commerce: OECD Recommendation

e. Where data protection laws are administered solely by data protection authorities (i.e. 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.

f. 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.

g. 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.

h. 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.

i. 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.

j. 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.

k. 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.

l. 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 consumers affected by algorithms underpinning digital financial services that can enable those adversely affected by the outcome to challenge it.

m. 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.

n. 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.

o. 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”).

References

Accenture (2017), Accenture Financial Services 2017 Global Distribution & Marketing Consumer study: financial services report, www.accenture.com/t20170111T041601__w__/usen/_acnmedia/Accenture/next-gen-3/DandM-Global-Research-Study/Accenture-FinancialServices-Global-Distribution-Marketing-Consumer-Study.pdf

Accenture (2019), Accenture Global Financial Services Consumer Study, https://www.accenture.com/_acnmedia/PDF-95/Accenture-2019-Global-Financial-ServicesConsumer-Study.pdf

Berg T., Burg V., Gombović A., Puri M. (2018), On the Rise of FinTechs – Credit Scoring using Digital Footprints, https://www.fdic.gov/bank/analytical/cfr/2018/wp2018/cfr-wp2018- 04.pdf Cormen T.,

Carnegie Endowment for International Peace (2020), Timeline of Cyber Incidents involving Financial Institutions, https://carnegieendowment.org/specialprojects/protectingfinancialstability/timeline

CIGI-Ipsos (2019), “2019 CIGI-Ipsos Global Survey on Internet Security and Trust”, www.cigionline.org/internet-survey-2019

European Commission (2015), Special Eurobarometer 423 Cyber Security - Report, http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

European Union (2016), Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation), https://eur-lex.europa.eu/legalcontent/EN/TXT/?qid=1532348683434&uri=CELEX:02016R0679-20160504

European Union (2015), Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, https://eur-lex.europa.eu/legalcontent/EN/TXT/?uri=CELEX:32015L2366

EU Financial Services Users Group (2016), Assessment of current and future impact of Big Data on Financial Services, https://ec.europa.eu/info/sites/info/files/file_import/1606-bigdata-on-financial-services_en_0.pdf F

Federal Trade Commission (2020), Consumer Sentinel Network, January 2020, https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-2019/consumer_sentinel_network_data_book_2019.pdf

Financial Conduct Authority (2019), Explaining why the computer says No, https://www.fca.org.uk/insight/explaining-why-computer-says-no

Financial Services Consumer Panel (2018), Consumer Panel Position Paper Consenting adults? - consumers sharing their financial data, https://www.fs-cp.org.uk/sites/default/files/final_position_paper_-_consenting_adults_-_20180419_0.pdf

Finextra (2019), Big Data in the Financial Services Industry – from data to insights, J Lochy, September 2019

G20 Global Partnership on Financial Inclusion (2018), G20 Policy Guide: Digitisation and Informality, https://www.gpfi.org/sites/gpfi/files/documents/G20_Policy_Guide_Digitisation_and_Informality.pdf

G20 OECD (2011), High Level Principles on Financial Consumer Protection, https://www.oecd.org/daf/fin/financial-markets/48892010.pdf

GSMA (2019), State of the Industry Report on Mobile Money 2019, https://www.gsma.com/sotir/wp-content/uploads/2020/03/GSMA-State-of-the-Industry-Report-on-Mobile-Money-2019-Full-Report.pdf

Hurley M., Adebayo J. (2017), Credit Scoring in the Era of Big Data, 18 Yale J.L. & Tech. Available at: https://digitalcommons.law.yale.edu/yjolt/vol18/iss1/5

IDC White Paper (2018), The Digitization of the World: From Edge to Core, https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf

Ipsos MORI (2019), UK Cyber Survey Key findings – General public, conducted on behalf on behalf of the National Cyber Security Centre and Department for Digital, Culture, Media and Sport (DCMS), https://s3.eu-west-1.amazonaws.com/ncsccontent/files/UK%20Cyber%20Survey%20-%20analysis.pdf │ 29

Joint Committee of the European Supervisory Authorities (2016), Discussion Paper on the Use of Big Data by Financial Institutions, https://esas-jointcommittee.europa.eu/Publications/Discussion%20Paper/jc-2016-86_discussion_paper_big_data.pdf

Merchant Savvy Data Hub, https://www.merchantsavvy.co.uk/mobile-payment-stats-trends/#

OECD (2007), Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy, http://www.oecd.org/digital/ieconomy/38770483.pdf

OECD (2013), OECD Policy Framework, https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

OECD (2014) Consumer Policy Guidance on Mobile and Online Payments, https://www.oecd-ilibrary.org/docserver/5jz432cl1ns7-en.pdf?expires=1605541040&id=id&accname=ocid84004878&checksum=19DBA345618E5F5A5531AE66432628B4

OECD (2015), Data-Driven Innovation: Big Data for Growth and Well-Being, https://read.oecd-ilibrary.org/science-and-technology/data-driven-innovation_9789264229358-en#page1

OECD (2016), Recommendation on Consumer Protection in E-commerce, https://www.oecd.org/sti/consumer/ECommerce-Recommendation-2016.pdf

OECD (2017), Robo-Advice for Pensions, https://www.oecd.org/pensions/Robo-Advice-for-Pensions-2017.pdf

OECD (2017), Technology and innovation in the insurance sector, https://www.oecd.org/finance/Technology-and-innovation-in-the-insurance-sector.pdf

OECD (2018), Financial Markets, Insurance and Private Pensions: Digitalisation and Finance, https://www.oecd.org/finance/private-pensions/Financial-markets-insurance-pensions-digitalisation-and-finance.pdf

OECD (2018), IoT measurement and applications, OECD Digital Economy Papers, No. 271, https://doi.org/10.1787/35209dbf-en

OECD (2018), Consumer policy and the smart home, OECD Digital Economy Papers, No. 268, https://doi.org/10.1787/e124c34a-en.

OECD (2020) Personal data use in financial services and the role of financial education, http://www.oecd.org/financial/education/Personal-Data-Use-in-Financial-Services-and-the-Role-of-Financial-Education.pdf

PwC (2017), Top financial services issues of 2018, https://www.pwc.com/il/he/bankim/assets/2018/Top%20financial%20services%20issues%20of%202018.pdf

www.oecd.org/finance