The Role of the Compliance Function in the Financial Sector in the Age of Digitalisation, Artificial Intelligence and Robotisation*

Gábor József Harkácsi – László Péter Szegfű

Our analysis is intended to fill a gap in the sense that the focus of our study is on the challenges of the compliance function and their responses, putting into complex perspective the lack of and the need for striking a delicate balance between the quality of the international and national legislative environments and the role of ethical and due diligence frameworks. As a result of digitalisation, FinTech enterprises have become unavoidable in the world of financial services, which has had the effect that the business and risk models of incumbent players have changed, exerting a strong influence on the regulatory environment and in parallel on the development and change of trust and reliability as well as ethical and prudent conduct. Inevitably, regulation will always fall behind new needs and new emerging technologies, since authorities need to develop a thorough understanding of the functioning and risks of these technologies in order to establish adequate regulation of them. The compliance function must find its place and role in this changing environment in order to be able to efficiently support financial sector participants in their duty to comply with rules and ensure fair and ethical conduct.

Journal of Economic Literature (JEL) codes: D18, D53, E58, G01, G21, O33, O52

Keywords: digitalisation, artificial intelligence, ethics, compliance, trust, banks, FinTech, PSD2

1. Introduction

A number of studies and articles have been published in international and national professional literature, examining the modern-day role of trust and ethics and seeking answers as to how trust, reliability, ethical norms and ethical conduct are changing in the FinTech space. These publications, including this paper, all confirm that the role of ethics is important, since it already provides a guide for control

* The papers in this issue contain the views of the authors which are not necessarily the same as the official views of the Magyar Nemzeti Bank.

Gábor József Harkácsi is a Senior Compliance Expert at the Magyar Nemzeti Bank. E-mail: harkacsig@mnb.hu
László Péter Szegfű is a Head of Division at the Magyar Nemzeti Bank. E-mail: szegful@mnb.hu

The Hungarian manuscript was received on 14 September 2020.

DOI: http://doi.org/10.33893/FER.20.1.152170

and accountability, even before comprehensive regulation of the FinTech space is completed. The studies also predict that the norms of ethics and conduct as well as the incomplete international regulations currently applied will be evaluated in the event of an economic slowdown or recession. Trust is fundamentally based on smooth cooperation, the experience of addressing issues together, ethical behaviour and a mutual moral commitment. In business relations, trust creates trust and the trust gained will create a presumption of reliability. Lack of trust, however, is detrimental and leads to a lack of willingness to cooperate and, ultimately, to damage to the business relationship. The role and responsibility of the compliance department in ensuring compliance and ethical behaviour, and thus in creating and maintaining trust and reliability, is extremely complex. On the one hand, as part of the internal control system of the organisation, it is responsible for identifying and managing organisational compliance risks.[1] On the other hand, a compliance department is not only an organisational unit or function, but also a complex system and a mental attitude that must be put into practice, throughout the entire organisation. Regarding the latter, organisational and functional independence along with firm support from top management and strong networking at the organisational level are necessary conditions.

The financial sector, and in particular the banking sector, has always operated on the basis of trust and consequently it has considerable experience in how to operate ethically and how to build up and maintain the trust of clients and the market; it also knows how quickly all of this can be lost. Rebuilding and regaining trust and reliability, as has become repeatedly clear after economic crises, is a slow and difficult process. Trust, reliability, ethics and good business reputation are valuable assets and at the same time they are tools for successful operation and profitability (*Müller – Kerényi 2019*).

The question, however, arises as to how ethical requirements, professional standards, applicable regulations change and transform when FinTech[2] players of the financial sector (hereinafter: FinTech) enter the financial services industry as enterprises that offer innovative financial solutions,[3] forcing traditional credit

[1] Compliance risk is defined as the risk of legal or regulatory sanctions, major financial loss or loss to reputation an institution may suffer as a result of its failure to comply with any laws, rules, regulations, guidelines of self-regulating bodies or ethical norms pertaining to its activity.

[2] Financial technology (hereinafter: FinTech) is an umbrella term for innovative products and services created in a digital environment and performed using digital devices with the aim of widening the range of services in new competition with financial services provided by the institutions of the financial sector (credit institutions, insurance companies, investment service providers, funds, other payment institutions, etc.), in order to make clients' use of the given service more convenient, faster and/or cheaper or to generate new client demands with an innovative approach. At the same time, FinTech also applies to a new industry that uses innovative technology to improve financial activities.

[3] FinTech enterprises are those actors that create FinTech applications for classical financial institutions, credit institutions, insurance companies, brokers, etc. or for the purpose of providing a separate service independently of them. FinTech applications include account information service providers (AISP) and payment initiation service providers (PISP) under PSD2, while they are commonly called third party providers (TPP).

institutions, banks, insurance companies and other financial institutions to transform their business models, not to mention that we also must respond to the challenges facing us, such as the consequences of the new coronavirus pandemic on digitalisation. Digital technologies are changing our lives: artificial intelligence, big data analytics, block chain and cloud-based technologies are improving our world in several ways, but while opening up new opportunities, they also bring new vulnerabilities, more scope for errors, and consequently previously unknown risks. The regulatory environment, however, will always fall behind the quick development of emerging new technologies, since regulators must first understand the practical functioning and risks of these technologies so that they can create adequate but not excessively restricting rules. The uniform requirements needed for an unimpeded building of the digital financial structure have been met only partially, and therefore, as a bridging solution, ethical and confidence requirements as well as business codes of conduct have been brought to the fore.

2. Threats and responses

The new technologies tend to bring considerable benefits worldwide, but they also pose risks. Major benefits include quick client acquisition, enhanced user experience, cost reduction, efficiency gains and a higher degree of transparency. Apart from this, innovation is an efficient tool to combat financial exclusion by offering high quality services to those who previously were not able to afford them. As one of the largest users of digital technologies, the financial sector plays a major role in the digitalisation of our economies and societies. FinTech enterprises providing financial services are breaking up a centuries-old monopoly in the field of traditional banking and financial services, opening up new channels for clients. Their entry to the market intensifies competition, but it also poses threats and new risks in addition to an aggravation of the already known operational and security risks, while their operation raises fundamental regulatory and social questions. The risks detected may worsen for several reasons. The main reasons include the fact that as a result of the emergence of a large set of new technologies in recent years and the open use of financial services (for example, open banking), the appearance of new services focusing on delivering user experience has quickly altered the dynamics of competition and business models have also changed at a more rapid pace. FinTech enterprises have the potential to penetrate the market of traditional financial services actively and more successfully, and the digital technologies applied in the course of providing their services – in particular where closely integrated into the operation of financial institutions and with access to sensitive customer data – have opened up a new dimension of operational risks. Access to customer data may generally occur through the Internet and through communication between interfaces, while the management, processing and storage of these data is mostly carried out through cloud computing services. As a result,

the technological solutions applied to services pose risks due to the nature of the Internet and due to the different security levels of the solutions provided by the many Internet user contractors involved in the service.

Taking all these risks into account and in particular the fact that FinTech enterprises usually provide their services managing cross-border and Internet-based services, it has been an essential step, in the interest of protecting the security of users, to tighten the standardised security requirements throughout European Union and to ensure a high level of consumer protection for the use of these services.

2.1. Tightening of the rules for payment services

The European regulator with the involvement of the European Central Bank (ECB) and the European Banking Authority (EBA), has developed a stricter regulatory framework for the provision of payment services, and thus on 12 January 2016, PSD2[4] entered into force and Member States had to transpose it into their national laws by 13 January 2018. In addition to the aim of ensuring effective protection for customers – especially for consumers – PSD2 was put into place to create a regulated environment for the development of digital financial services, to support new providers including those without a credit institution background in entering the financial services market and to further increase the security of payments in view of the growing expansion of online transactions. At the same time, PSD2 opens up huge opportunities for FinTech players, also called third party providers, by granting them access to their customers' payment accounts. The task of ensuring the protection of customers' personal data falls under the scope of the General Data Protection Regulation (GDPR[5]) and the respective national legislation. Protection of data that qualify as a financial sector secret is regulated by the respective laws of the financial sector, while regulation relating to sensitive payment data is set out in the additional provisions[6] of the Act on Payments Services.[7] Under PSD2 and payment regulations transposing PSD2 into national law, in the course of providing their services, third party providers can access their customers' payment accounts data subject to the consent of the customer and to the extent that it is absolutely indispensable for providing the service.

[4] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC

[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[6] Under section 2 (5a.) of the Act on Payments Services, sensitive payment data means data, including personalized security credentials which can be used to carry out fraud with the provision that in respect of payment initiation services or account information services, the name of the account owner and the payment account number do not constitute sensitive payment data.

[7] Act LXXXV of 2009 on the Pursuit of the Business of Payment Services

2.2. Strengthening the protection of data

According to the provisions of the respective laws, it is typically the responsibility of the service provider to ensure the proper protection of customer data. By providing for severe sanctions, adoption of the GDPR has further tightened the already strict approach of financial institutions towards data protection and data security. Unfortunately, the GDPR only applies to personal data, and thus service providers sought to tailor their rules and solutions for data protection and data security to the personal data of their customers, paying no attention at all to the fact that service providers may access other sensitive data, only some of which fall within the category of personal data.

In order to ensure proper data security, it is indispensable that market participants conduct a comprehensive assessment of the data assets they manage, including – in addition to personal data – data classified as secrets by the respective laws of the financial sector, trade secrets, data that are publicly available but to be actually protected, and sensitive data for which there is no legal regulation but may affect the proper functioning, security or even the market position of the institution. Data and data management systems must be classified into different security categories. The three main pillars of information security are confidentiality, integrity and availability. It is also necessary to assess the risks for the information security categories and to take adequate measures to address these risks, taking into account the respective legal provisions as well as the respective ethical and social expectations and norms.

2.3. Customer due diligence; opening and regulation of new possibilities for remote contracting

The increasingly stringent anti-money laundering directives and regulations of the EU,[8] along with the AML Act transposing them into national law and the MNB Decree[9] on its implementation provide fundamental guarantees necessary to protect the integrity of the European financial system against money laundering and terrorist financing. In addition, the AML Act and the respective MNB Decree opened up new possibilities for the rise of innovative financial technologies. In some cases, particularly where institutions falling under the effect of the Act[10] establish relations with new customers,[11] service providers are required to execute the so-called customer due diligence. Already at the time of entry into force in 2017, this

[8] The MNB offers a collection of links to the respective norms on its website: https://www.mnb.hu/en/supervision/regulation/anti-money-laundering/requirements-and-guidance/eu-regulations
[9] MNB Decree 26/2020 (VIII.25.) on the detailed rules concerning the implementation of the Act on the Prevention and Combating of Money Laundering and Terrorist Financing, as applicable to service providers supervised by the MNB, and concerning the minimum requirements for the development and operation of the screening system under the Act on the Implementation of Restrictive Measures Imposed by the European Union and the UN Security Council Relating to Liquid assets and Other Financial Assets MNB Decree
[10] Section 1 (1) of the AML Act
[11] Section 1 (6) of the AML Act

Act opened up the opportunity for remote customer due diligence carried out in electronic form through audited electronic communications equipment. The Act authorised the MNB to specify the technological details. At the beginning, the MNB Decree preferred customer due diligence via video chat, the closest to personal appearance, while later it permitted several selfie-based identification solutions. The most recent version of the Decree allows the use of identification cards equipped with an electronic storage unit and the use of travel documents with an integrated chip containing biometric data for the identification of customers in respect of customer due diligence carried out for the purpose of preventing money laundering, which may significantly facilitate the remote acquisition of customers. As meanwhile the requirements of the written form under the Civil Code have been simplified, the MNB concluded that if the customer makes a legal declaration in the course of the customer due diligence process carried out for the purpose of preventing money laundering through audited electronic communications equipment and the service provider ensures unchanged quote of the legal statement, it will comply with the written form requirement of contracting. As a result, the process of remotely acquiring customers can run fully online without interruption even in cases where the law prescribes the written form. This offers significant support to FinTech players in customer acquisition.

3. Responsibility of regulatory actors

The responsibilities of the regulatory actors are twofold: on the one hand, they are of a supportive nature; on the other hand, they must consider security and other risks. They must ensure that legal constraints do not form barriers to the spread of new technologies and business innovation, and at the same time they must facilitate the entry of new market players, ensuring fair competition in a way that new players are not placed at a competitive disadvantage and the interests of traditional financial institutions are not affected either – and naturally all of this should be done with the security risks in mind. From a regulatory standpoint, it is also important to take into account the fact that the usability and the security of certain innovations are in inverse proportion to each other. Regulators must strike a balance that does not yet pose obstacles to the usability of solutions, but still provides enough security to preserve the financial stability of financial institutions, customers and Member States. It is, however, a major challenge for legislators to be able to follow the rapid technological development by establishing and amending the respective legislations, and under these circumstances compliance with and enforcement of ethical norms has a key role to play.

4. Trust, reliability, compliance and ethics in the digital world

4.1. Rapid development

Technology has progressed extremely rapidly, making a significant impact on our everyday lives, and the task of keeping pace with this rapid development presents a significant challenge for legislators as well. The change affected the financial sector in an exceptional way: in many cases banks were pioneers in applying new technologies which led to a reduction in their costs and at the same time to increased satisfaction among their customers. The vast majority of users welcome FinTech services, because the service is fast and much cheaper than traditional financial services, particularly the services requiring personal presence. However, the level of suspicion and the risk sensitivity of users with regard to the services – primarily among the young due to the insufficient information at their disposal – is rather low. The main motivations are convenience, quickness and cost saving. Banks are also constantly adapting to new technological opportunities and as a result their customer service is increasingly shifting towards electronic, in particular, Internet-based communication. Additionally, they are striving to keep up with FinTech firms by providing similar value-added services that focus on delivering user experience. In addition, the coronavirus pandemic has provided fresh motivation, and the measures taken in consequence have explicitly speeded up digitalisation. Within a short time, the financial sector switched to almost fully digital operations, in the context of which the scope of functions and services available through internet and mobile banking has widened. At the same time, the number of those customers – including all age groups, but mainly the elderly – who make use of these services in order to avoid having to personally visit a bank branch has increased significantly. In order to secure and retain the benefits offered by digitalisation, digital financial services providers utilise every available piece of digital technology for the provision of their services in the course of their operation, such as application programming interfaces (API), artificial intelligence, data analysis methods, robotics and the use of data collected or left behind. These data are collected and recorded through algorithms and programmed applications, and service providers provide their services or a part of their services in return for these data. They sell the data or use them for the provision of other services sold for money, which generates revenue. All of this has led to extremely rapid development whereby, with the variety of their services, the ever-growing FinTech enterprises represent and cover such a wide range of financial services that legislators find it rather difficult to keep up with the pace as regards the amendment of the currently effective and applicable legislations or the creation of new legal provisions. For this reason, it is particularly important that there be strong ethical norms. Developments and innovations should ensure consistent value enhancement for customers, while they are treated in a fair and ethical way.

4.2. Appropriate regulatory environment

One essential condition for development is to create and maintain an international and national regulatory environment which supports useful and valuable innovations, and at the same takes efficient and firm action against overly risky, unethical or harmful conduct (*MNB 2019*). Legal provisions, regulations and supervisory bodies must adapt to innovation and find the right balance between supporting and regulating innovation. Financial technology requires a balanced approach between regulation of the institution and regulation of the activity. This is necessary because, as a consequence of the complex interaction between technology and regulation, contradictions may arise. For example, it may happen that certain companies and service providers are regulated differently even if they carry out basically the same activities. Moreover, the current regulation takes the wrong approach to certain activities in terms of definition and/or scope of activities. The existing EU legislation is overly complex since a number of overlapping provisions relating to FinTech innovations are in force. In order to avoid placing FinTech players in a situation of competitive disadvantage, but at the same time to make sure that the interests of traditional credit institutions are preserved, it is necessary to ensure a standardised regulatory environment across the European Union. Regulation, however, is not yet complete; the procedure is still in progress. The next section presents the important areas where the regulation in force should be improved or supplemented.

4.2.1. Liability rules pertaining to new technologies

The question of legal liability is an issue that still needs further clarification. In the course of developments – such as customer risk analysis using AI technology, fraud monitoring, robo-advice, big data analysis – errors and distortions inherent in technology may even lead to a systemic risk and may cause harm to customers. However, it is not clear who bears the legal liability in such cases. Trustworthy artificial intelligence must comply with the effective laws and regulations. Determining liability is a serious issue, also because the working of the technology is not evident: it is based on algorithms which are not exclusively written by human beings. Furthermore, it is complex, unpredictable, non-transparent, and therefore when making its own decisions, it is not always possible to identify precisely where, how and why a potential mistake or error could have happened. For this reason, serious resentments have emerged against the technology. When setting up legal frameworks, it is important that the legislator minimise the risks posed by AI to the extent possible in a such way that sectoral specificities such as sectoral laws are taken into account. Regulation should prefer a people-centred approach and should protect the individual from possible asymmetries in automatic decision-making and help enterprises developing and implementing AI technology by providing legal certainty. It should not create competitive disadvantages or excessive administrative burdens and it should not hamper the appropriate development of technology.

At the same time, it should be technologically neutral and should consider international standards and regulatory frameworks. The EU has recognised that from the aspect of promoting European values, it is important that regulatory and ethical principles are defined at the EU level, and it laid down a high level European Union strategy for artificial intelligence,[12] in addition to setting out the principles in its White Paper on artificial intelligence (*European Commission 2020*). With the purpose of laying down Hungary's national regulation on AI, the Hungarian Artificial Intelligence Coalition was established on 9 October 2018 with the participation of 78 international and Hungarian companies together with universities, scientific workshops, professional and administrative organisations.[13]

In addition to the regulation of AI, the entry into force and application of PSD2, the AML Directives, the NIS Directive,[14] and the GDPR marked the start of the establishment of a necessary standardised European regulatory environment. As part of this process, European guidelines have been and are being specified on several topics, such as the use of cloud computing services and the application of artificial intelligence. This is important also because the management and processing of the sensitive data of customers and partners – in respect of both FinTech and incumbent players – is increasingly carried out by cloud computing applications and by systems relying on AI tools. Credit institutions and FinTech enterprises store and use the identification data, account number, payment transaction data and other personal data of their customers in order to provide personalised services to their customers. However, in order to ensure the proper protection of customer data, the responsibilities and competences of the data owner in respect of the entire process should be clearly defined. Compliance with the principles of data protection set out by the data owner must be enforced technologically or through the application of legal safeguards during the entire process, independently of whether data management or data processing is carried by different players. Artificial intelligence which supports the use and utilisation of data or optimises decision-making relating to data or based on data extraction, machine data analytics and robotics are already inseparable tools of the digital financial services and – as discussed above – it is the associated risks and prejudices that cast the most enormous shadow over FinTech solutions. This is where the requirement of trust and ethics is most apparent, since regulators primarily seek to regulate the FinTech services themselves, and it is more difficult to identify the technologies and tools used by these services and properly regulate the functioning thereof. According to the legislative intent, just as under PSD2, the duration of financial services provided by FinTech enterprises lasts until, for example, a FinTech enterprise providing account information services

[12] Artificial Intelligence for Europe, COM/2018/237 final
[13] https://digitalisjoletprogram.hu/en/content/artificial-intelligence-coalition
[14] https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

forwards or makes available to the customer the data requested by the customer. Of course following this, customers may freely dispose of the data provided within the framework of the service, and for example with the acceptance of the service provider's condition that for the sake of the free use of the service, FinTech enterprises may transmit data collected by them to a third party (e.g. to accountants, to marketing companies to carry out targeted advertising or financial institutions providing loans to make personalised credit offers or to propose loan facilities), the further fate of the data, and the way the data is processed and used by a third party is less regulated, and thus less transparent and controllable. This data transmission cannot be considered as a service provided within the framework of the account information service, for example under law,[15] and thus the rules of PSD2 cannot be applied. Therefore, in the course of data transmission falling outside the scope of the service, FinTech enterprises must consider, besides the legislation governing data protection and more specifically the rules of the GDPR – among other things – the statutory provisions relating to the transmission of data classified as secrets by the laws of the financial sector (such as bank secrets under the Credit Institutions Act or payment secrets under the Payment Services Act[16]). In addition, it is also necessary to examine the application of rules on outsourcing and, in the light of the existing legal loopholes, the norms of ethics, behaviour, conduct and due diligence.

4.2.2. Identical activities, identical regulation

Based on feedback from the market, there is still no level playing field, since PSD2 leads to a large loss of data and market share for the banking sector if banks themselves do not launch costly digital developments. Third party providers experience distortion of competition in several respects as well. Although connection is made via open interfaces based on standard protocols, both third party providers and banks providing such services need to implement developments entailing significant costs for each connection. The costs and durations of these developments and the need to connect banking interfaces of various parametering, i.e. interfaces that are based on different standards[17] instead of a single, uniform standard and contain country-specific elements[18] raise the barriers to entry and slow down the introduction of new services to be provided by the banking sector under PSD2. Besides all of this, in order to avoid presumed or real loss of market, certain credit institutions are trying to hamper or restrict the ability of third party providers to connect by imposing mostly unethical but in some cases unlawful conditions or testing circumstances or procedures on the pretext of handling incidents that may have occurred. In an effort to facilitate a common interpretation of "obstacles" and

[15] Section 6 (1)101a. of the Credit Institutions Act
[16] Act CCXXXV of 2013 on Certain Payment Service Providers
[17] The two largest are Berlin Group and Open Banking
[18] E.g. special fields required for instant payment service in Hungary

the application of laws in relation to disputes, the EBA published its opinion[19] to clarify the definition and examples of obstacles under Article 32 (3) of the RTS on SCA and CSC,[20] and the MNB also published its tool of supervisory regulation on the secure communication relating to services provided by third party providers.[21]

With regard to the risks arising from services, FinTech enterprises including the operation of third party providers are subject to licensing or registration requirements in any case. With a view to enforcing identical principles, providers must go through a strict licensing procedure, but this does not mean that authorities hinder or impede the market entry of providers intending to operate with proper guarantees. When issuing licenses in Hungary, in order to ensure compliance with the strict conditions, the MNB offers a number of opportunities for facilitating licensing. To this end, it published a detailed guide[22] and a summary of frequently asked questions[23] and facilitates the market entry of new financial solutions via other supervisory innovations.

4.2.3. Strong customer authentication

Another fact that represents a considerable competitive disadvantage for third party providers is that the EBA provided the national supervisory authorities of the Member States with the opportunity to extend the deadline for banks and other payment service providers to comply with the legal provisions on strong customer authentication until 31 December 2020 concerning e-commerce card-based payment transactions, but at the same time, third party providers were not given the opportunity to omit the application of strong customer authentication in the course of the provision of their services. PSD2 set the date at 14 September 2019 from which banks and other payment service providers – in order to provide customers with online access to payment accounts or to electronic payments – must apply the provisions on customer authentication requiring the application of strong, at least two-factor authentication (for example PIN code and fingerprint or a password and SMS code). However, taking into account the complexity of the regulation as well as the request and lobbying activity of card issuers and merchants, the EBA, as coordinator of the work of the national supervisory authorities, allowed the supervisory authorities of the Member States to provide additional time for completing IT developments and migrating to the new customer authentication

[19] https://eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2020/884569/EBA%20Opinion%20on%20obstacles%20under%20Art.%2032%283%29%20RTS%20on%20SCA%26CSC.pdf
[20] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication
[21] https://www.mnb.hu/letoltes/vezetoi-korlevel-a-fizetes-kezdemenyezesi-es-szamlainformacios-szolgaltatasokhoz-kapcsolodo-biztonsagos-kommunikacioval-2020-07-13.pdf
[22] https://www.mnb.hu/felugyelet/engedelyezes-es-intezmenyfelugyeles/engedelyezes/szektorok/penzpiac/penzforgalmi-intezmeny/kizarolag-szamlainformacios-szolgaltatast-vegzo-penzforgalmi-intezmeny-bejelentese, https://www.mnb.hu/letoltes/penzforgalmi-intezmenyek-tevekenysegenek-engedelyezese.pdf
[23] https://www.mnb.hu/penzforgalom/psd2-gyakori-kerdesek-es-valaszok/engedelyezes

procedures relating to e-commerce card-based payment transactions until 31 December 2020. During this transition period, customers of banks and other payment service providers were allowed to use their payments cards for online domestic and cross-border payments without the application of strong customer authentication.

4.2.4. Fraud prevention

The opportunities offered by digital technologies, open banking and instant payment essentially brought about a paradigm shift that led to the alteration of the related risks, such as the risks of fraud. The involvement of various actors makes the system more complex, meaning that payment transactions are now executed with the joint participation of 5-6 actors, all being potential target, and thereby constituting potential new vulnerable points or targets for attacks. This may lead to the alteration of the risks of fraud and the emergence of other, currently hidden risks. The increase in these risks may cast a shadow over FinTech, and therefore it is vitally necessary for the regulatory environment to be adaptable to this change. Although PSD2 and the related RTS on SCA and CSC provide that a modern monitoring system must be operated for the detection of unauthorised transactions and fraudulent payment transactions, the application of this requirement in real time is only mandatory under certain conditions.[24] This, however, means that the risks of the so-called instant fraud[25] arising from the peculiarities of instant payment are only partially addressed. A modern monitoring system must be able to analyse activity and device risks for all users (including third party providers) and of each digital channel in real time (taking into account that instant payments are executed in just a few seconds) and it must respond to suspicious events and known fraud scenarios. However, considering the requirements of the RTS on SCA and CSC, the operation of a monitoring system in real time is currently not a statutory provision of general application.

A modern monitoring system must also be able to hold its ground in a crisis situation. The coronavirus came as a new shock to the world economy and the financial sector had very little time to react. As the population was forced into lockdown, it was necessary to switch to almost fully digital operation, in the context of which the scope of functions and services available through Internet and mobile banking has widened. As discussed above, the clientele that makes use of these services in order to avoid making a personal visit to a bank branch has also grown. However, a significant risk is posed by the fact that many of these new customers, particularly the elderly – who are at the highest risk from the coronavirus

[24] Based on transaction risk analysis, a remote payment transaction can be considered as low risk and the use of strong customer authentication is not required.
[25] The risk relates to the fact that the money is transferred to the fraudster within 5 seconds, and therefore the prospects of recovering the stolen money are minimal.

– have never used digital banking services in the past, and therefore criminals can easily exploit and do exploit the lack of knowledge and experience. With the development of digital technologies, fraud is becoming increasingly sophisticated and, amid coronavirus pandemic, the number of fraud attempts and the frequency of successful fraud have also increased globally (*Javelin Strategy & Research and SAS 2020*). The increased number of transfers and card not present (e.g. online bankcard payments) resulting from the growing clientele – together with the fact that the previously offline generation has lower levels of knowledge in the field of digital banking services – puts a heavy additional burden on the compliance departments of financial institutions concerned to prevent fraud and abuse. It is particularly problematic that fraud detection and prevention is a special area that still has limited available competences. Fraud detection systems also increasingly apply solutions of artificial intelligence and although they prove to be efficient, they raise several regulatory-related questions, such as, from the perspective of data protection, forbidden accumulation of data, profiling subject to strict requirements, compliance of targeted data processing, provisions on data storage or processing of data falling within the scope of sectoral secrets. Account should also be taken of the fact that, besides the compliance and ethical issues in relation to solutions supported by artificial intelligences discussed above, the storage and processing of data is mostly carried out through cloud computing services, which may raise further data protection, confidentiality and ethical concerns.

4.2.5. Outsourcing and the use of cloud computing services

While offering the advantage of cost-efficiency and ease of use, cloud computing services which are becoming increasingly popular among financial institutions and third party providers involve a number of risks, including – but not limited to – the inherent element of service models that service providers offer the same or similar services to different institutions, and therefore it is necessary to ensure that data is separated in a proper and secure way. It is important that not only other users of the services, but also the very service provider or its contractors should be prevented from gaining access to data, except where control measures are taken – under a contract – and the participants involved are only allowed to handle data as specified in the contract. Another risk to be highlighted is the exit strategy, since – primarily in the Software as a Service (SaaS) model – the institution may lose control over the processing of their data as well as over the proper possession of processed data and the further possibilities of data processing.

Be it the outsourcing of single solutions or the infrastructure to an external service provider, it is necessary to focus in all cases on compliance with the respective EU, national, sectoral laws and supervisory regulatory norms. The term of outsourcing is defined differently in Hungary's national legislation and in EU legislation: in Hungary's laws the term of outsourcing is distinguished from the general

subcontracted activities. Unfortunately, sectoral laws give different meanings to the term "outsourcing". The Credit Institutions Act, the Investment Firms Act,[26] the Act on Voluntary Mutual Insurance Funds[27] and the Act on Private Pension Funds[28] link outsourcing to data management and impose strict contractual requirements on institutions, while, for example, under the Act on Payment Service Providers[29] or the Insurance Act,[30] outsourcing is the activity that could be undertaken by the institution but is performed by an external service provider under a contract. Besides, the Collective Investment Undertakings Act[31] explicitly excludes the development of IT systems and the operation and maintenance of IT systems from the scope of outsourcing. In respect of the application of legal requirements for outsourcing, the MNB provides guidance in its supervisory regulatory tools.[32] The use of cloud computing services mentioned above – provided it complies with the respective provisions of sectoral laws – must also be treated as outsourcing, but in the course of the use of this service, special attention should be paid to the specificities of the technology. In respect of the applicable norms, the MNB provides guidance in a special supervisory regulatory tool.[33]

However, independently from the fact whether the use of third party providers is through outsourcing or subcontracting, institutions are required to exercise due care and comply with ethical, moral and prudential norms – particularly where the use of third party providers includes customer data or communication with customers – even though these norms are not based on legal requirements.

4.3. Confidence building, fair and ethical behaviour

4.3.1. The ways to build trust and reliability have changed

Trust, reliability, ethical conduct together with good business reputation are expectations and professional requirements, compliance with which has value, and they also form the basis for successful operation and profitability. As regards

[26] Act CXXXVIII of 2007 on Investment Firms and Commodity Dealers, and on the Regulations Governing their Activities
[27] Act XCVI of 1993 on Voluntary Mutual Insurance Funds
[28] Act LXXXII of 1997 on Private Pensions and Private Pension Funds
[29] Act CCXXXV of 2013 on Certain Payment Service Providers
[30] Act LXXXVIII of 2014 on the Business of Insurance
[31] Act XVI of 2014 on Collective Investment Trusts and Their Managers, and on the Amendment of Financial Regulations
[32] MNB Recommendation 7/2020 (VI.3.) on the usage of external service providers is directly applicable to outsourcing, MNB Recommendation 27/2018 (XII.10.) on setting up and using internal lines of defence and on the management and control functions is applicable to inspection duties, while MNB Recommendation 8/2020 (VI.22.) on the protection of information systems discusses the management and monitoring of IT outsourcing in separate chapters.
[33] In terms of managing cloud computing specific risks, the MNB expects the application of Recommendation 4/2019 (IV.1.) on the usage of community and public cloud computing services which includes the recommendations the European Banking Authority on outsourcing to cloud service providers of 20 December 2017 (EBA/REC/2017/03 https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2170125/e02bef01-3e00-4d81-b549-4981a8fb2f1e/Recommendations%20on%20Cloud%20Outsourcing%20%28EBA-Rec-2017-03%29_EN.pdf?retry=1). Although the EBA repealed the recommendation on cloud outsourcing, it incorporated the requirements formulated in the Recommendation into its Guidelines on outsourcing arrangements (EBA/GL/2019/02)

FinTech enterprises, in the initial period, there was no particular need to build trust, and regulation was loose and permissive. With the advent of Internet and digital technologies, the ways to build trust and reliability have changed. Trust and reliability increasingly tend to be the outcome of communication between customers as well as recommendations by other customers and their network of personal contacts. However, the increasing number of complaints about phishing or about the collection, management and use of personal data, primarily handled in the course of the provision of a service or left behind, that is not even known to the user of the service, who is also the owner of data, highlights the drawbacks of FinTech services and the risks related to the use of these services. FinTech enterprises are creating exciting new products and value-added services in response to customer needs, utilising technologies, such as artificial intelligence, robotics and machine learning. Traditional credit institutions have also initiated innovative developments, and they have established several types of partnerships with service providers emerging in this field, or have simply acquired the novel solutions together with the FinTech start-ups themselves, integrating them into their own operations. Digital technologies and now also open banking coupled with the opportunities offered by instant payments have altered the risk profile of traditional credit institutions as well. It is therefore important that regulation by virtue of legal provisions alone is not sufficient: it is also necessary to set requirements for fair and ethical conduct. In order to manage the changed risk profile, in addition to an efficient regulatory environment, we need an efficient compliance and internal audit programme. An appropriate and continuously maintained compliance and internal audit programme can provide a solution for exploring new, potentially hidden threats and managing the identified risks in a proper way. The key pillar of an atmosphere of confidence and reliability is the prudent and ethical operation which, however, requires the commitment of the management, and it is also vital to make sure that employees know and comply with the respective legal provisions, rules and ethical norms. This can be achieved primarily by improving awareness and providing continuous information and education, and by executing periodical – planned – audits. It is an example of exemplary practice, if the compliance department, in fulfilment of its consultative, guidance and preventive duties, can provide, on a continuous basis, satisfactory responses to the relevant questions of employees either personally, on the phone, through electronic channels or, in certain cases, anonymously, for example acting as a whistleblower. However, it should also be taken into account that FinTech enterprises utilise every available piece of digital technology for the provision of their services, and therefore norms of ethical conduct must be determined and enforced not only in relation directly to FinTech and digital financial services providers, but they must imperatively be extended to cover the tools, technologies and solutions indispensable for their activities, thereby regulating the

toolbox of FinTech and BigTech financial services, including for example artificial intelligence and the use of data managed or left behind within big data.

4.3.2. Development of ethics and due diligence frameworks

When formulating and implementing a compliance programme, in addition to ensuring compliance with legal requirements, the compliance department must also pay particular attention to the duty of care. This obliges compliance departments to monitor not only whether enterprises, in the course of their activities, comply with the effective laws, but also whether what they do is right and that the requirements of trust, reliability and ethics are also not compromised. In this context, it is an important compliance task on the one hand to promote an ethical culture, keeping the management and employees informed about what is right and what is not acceptable and on the other hand to establish the foundations for raising compliance awareness and to familiarise employees with these foundations. Recognising the risks faced by the intermediary system and money markets, there is a process underway in parallel with the elaboration and the implementation of the necessary legislation to develop ethics and due diligence frameworks, extending the norms to FinTech enterprises and to the tools used by them. In April 2019, the European Commission published a document entitled "Ethics Guidelines for Trustworthy Artificial intelligence" (*European Commission 2019*) with the aim of promoting the use and development of trustworthy artificial intelligence.

Trustworthy AI displays three components which should be ensured throughout the system's entire lifecycle: it should be lawful, complying with applicable laws and regulations; it should be ethical, ensuring adherence to ethical principles and values; and it should be robust, both from a technical and social perspective, since, even with good intention, AI systems can cause unintentional harm.

Laws are not always up to speed with technological developments: at times they can be out of step with ethical norms or may simply not be well suited to addressing certain issues. However, for AI systems to be trustworthy, they should also be ethical, ensuring alignment with ethical norms.

4.3.3. Prudent, ethical conduct towards customers

The application of ethical procedures towards customers plays an ever more prominent role these days. The role of consumer protection authorities is increasingly strong and as a result trust in the financial intermediary system and its supervision is gradually increasing. Customers may contact supervisory authorities with their complaints – if they do not receive a satisfactory response from the financial service provider – and submit a customer protection complaint in individual cases, or a public interest disclosure in case of infringement or systemic

problems affecting other consumers[34] as well. Disputes between consumers and financial institutions can also be settled out of court via the forum of Financial Arbitration Board.[35]

A condition to be satisfied for prudent operation is the provision of appropriate, comprehensive information to customers already prior to contracting, in due time and in a verifiable way. There are several legal provisions pertaining to the obligation of providing information to customers, from data management to the creation of conditions for proper decision making relating to the use of the service, however laws do not cover every issue here either, and therefore diligent, ethical and prudent conduct has a special role in providing adequate information to customers.

Besides the rules of the GDPR, the respective sectoral laws also include provisions on data management. In the case of using outsourcing services, credit institutions must inform their customers, also in the standard service agreement, on who may access sensitive data in the course of data processing.[36] Although there is no legislative requirement to do so, the fair practice of an institution includes making the entire outsourcing chain transparent to customers.

Consumer protection requirements under the respective law[37] protect customers that qualify as consumers. A key ethical question is that customers not qualifying as consumers should also receive similar protection in the context of the applied procedures.

With a view to facilitating the application of respective legal provisions and laying down prudential expectations, the MNB published a tool of supervisory regulation.[38] Since neither the legislative nor the regulatory norms can be fully comprehensive, institutions must provide for fair and acceptable procedures, apart from the legal obligations. A further expectation is that institutions should consider themselves to be bound by the respective codes of ethics and conduct as well as decisions made by the Financial Arbitration Board.

The principles of fair procedure include the principle of ensuring the use of services for all persons with disabilities through appropriate technical solutions, and as far as possible in standard quality, providing the same level of customer experience.

[34] According to the provisions of Act CLXV of 2013 on Complaints and Public Interest Disclosures and to Act CXXXIX of 2013 on the Magyar Nemzeti Bank
[35] https://www.mnb.hu/en/hungarian-financial-arbitration-board
[36] According to the provision of Section 68 (12) of the Credit Institutions Act
[37] Act XLVII of 2008 on the Prohibition of Unfair Commercial Practices against Consumers
[38] MNB Recommendation 10/2016 (X.24.) to financial organisations on the application of consumer protection principles

5. Conclusions

Up to now, the requirements needed for the smooth building and development of digital financial infrastructure have been met only in part, and thus, as a bridging solution, ethical and confidence requirements as well as business codes of conduct have been brought to the fore. Compliance departments in companies operating in the financial sector have a crucial role to play, since due to the incomplete state of the regulatory framework, this is the area which is tasked with ensuring compliance with legal provisions and other applicable recommendations, ethical norms, guidelines and guidance and with identifying and addressing compliance risks inherent in the activities of an organisation. It is not enough only to monitor whether the provision of services complies with the effective laws, but it is also necessary to monitor that requirements of trust, reliability and ethics are not compromised. This task is made more difficult given that a compliance department has to hold its ground in a continuously changing and developing regulatory environment in a period where the consequences of the coronavirus pandemic affecting economic and financial life have reached the digital world, too. However, just as every crisis, the current one caused by the coronavirus pandemic, whilst carrying significant risks, presents an opportunity. Social distancing rules introduced as precautionary measures have moved many activities into the online space, as a result of which consumer behaviour has drastically changed, facilitating the digitalisation of processes. Also in Hungary, digitalisation has been considerably encouraged by the quick and efficient answers given to the coronavirus pandemic situation and to the inherent difficulties, and that response has also strengthened the country's competitiveness in the longer term. Numerous new digital services have been introduced, and the measures taken as a result of the pandemic have explicitly speeded up the emergence of digital projects. In particular, limitations on customer services rendered through physical presence and on customer service performed in bank branches have contributed to a quicker development of options for digital contracting, remote customer identification and electronic payment. Within a short time, the financial sector switched to an almost fully digital operation, in the context of which the scope of functions and services available through electronic customer channels (on web-based and mobile platforms) has widened and at the same the clientele that makes use of these services has also grown. Besides the aspect of convenience, this is due to the efforts to reduce pandemic risks through measures to limit personal interactions. However, a significant risk is posed by the fact that many of the new customers, particularly the elderly who are at the highest risk from the coronavirus, have previously not used digital banking services, and therefore criminals can easily exploit their lack of knowledge and experience. Although the younger generations favouring FinTech services have well-developed digital and online skills and believe in quick, cheap and convenient payment solutions, their financial and security awareness is not in line with their skills, and thus they are also

faced with the risk. Apart from the risk posed by the lower level of knowledge of the previously offline generation in the field of digital banking services, the increased number of transfers and card not present transactions (for example online bankcard payments) also puts a heavy additional burden on the compliance departments of the financial institutions concerned in fraud and abuse prevention which serves the interest of both the banks and the customers.

Due to the development of digitalisation, robotisation and artificial intelligence and due to the emergence of economic and financial problems resulting from crises, in this case from the coronavirus pandemic, regulators must continuously respond to new risks. As mentioned above, regulation – necessarily – will always fall behind new needs and new emerging technologies, since the authorities need to develop a thorough understanding of the functioning and risks of these technologies in order to establish adequate regulation of them. And, in any case, rules – as the saying goes – are valuable only to the extent we can follow them. The role of ethics is therefore crucial in the global world, because the rules of co-existence satisfactory to all must be planted into the thinking of society along with ethical principles and objectives. For a global world, we need to formulate, establish and apply ethics that go beyond individual interests and economic profit maximisation in a modern sense. The objective must be to ensure a decent standard of living, security and sustainability for the whole of humanity and in order to achieve this the compliance department must be ready to perform its respective tasks.

References

European Commission (2019): *Ethics Guidelines for Trustworthy AI*. https://op.europa.eu/en/publication-detail/-/publication/d3988569-0434-11ea-8c1f-01aa75ed71a1/language-en

European Commission (2020): *White Paper On Artificial Intelligence – A European approach to excellence and trust.* https://op.europa.eu/en/publication-detail/-/publication/ac957f13-53c6-11ea-aece-01aa75ed71a1. Downloaded: 8 February 2021.

Javelin Strategy & Research and SAS (2020): *The Escalation of Digital Fraud: Global Impact of the Coronavirus.* https://www.javelinstrategy.com/sites/default/files/files/reports/20-5010J-FM-The%20Escalation%20of%20Digital%20Fraud-SAS_0.pdf

MNB (2019): *FinTech Strategy.* Magyar Nemzeti Bank. https://www.mnb.hu/letoltes/mnb-fintech-strategy-eng-cov.pdf

Müller, J. – Kerényi, Á. (2019): *The Need for Trust and Ethics in the Digital Age – Sunshine and Shadows in the FinTech World*. Financial and Economic Review, 18(4): 5–34. http://doi.org/10.33893/FER.18.4.534