

## The Darker Side of Fintech: the Emergence of New Risks

*Željko Jović\**  
*Ivan Nikolić\*\**

**Abstract:** The financial sector has always been recognized as a traditional activity. One of the biggest challenges facing the financial sector recently is the introduction of new technologies. Financial innovations, and especially the development of financial technologies (FinTech), contribute to changing the way the entire financial system, including the banking sector, changes in the digital economy. The changes brought about by financial innovations and technologies condition all market participants, and especially banks, to continuously improve their business in order to keep up with the competition. FinTech enable easier access to financial services, improvement of traditional services, provide greater efficiency, lower costs and automation of regulatory reporting. They have changed the way we perceive financial institutions. Banks can increasingly be seen as an application on the phone and computer through which financial services can be performed, less and less as a grand building that instils confidence. However, it should be borne in mind that the application of financial innovations, in addition to the advantages, carries with it many risks, in a way that it can be said that digital technologies change existing ones, but also bring new risks in the field of financial services. The key risks caused by these technologies include strategic, operational and cyber risk, the risk of business compliance with data protection regulations, as well as liquidity risk. The importance of outsourcing risk is not negligible. It is precisely because of the speed of change and innovation that new risks are constantly emerging. With the growing importance and number of these firms, as well as the speed of their cross-border transactions, the fact is that it is necessary that these firms must adjust the way they measure risk in accordance with the speed and pace of their development. The importance of risk management must be one of the key points for FinTech companies, both now and in the future. Due to the observation of advances in financial technologies and the assessment of the risks that financial innovations bring, there is a need to harmonize regulatory frameworks, in order to ensure that none of the financial service providers would be at a disadvantage. However, regulatory bodies must carefully consider the dynamics and manner of regulation, bearing in mind that in a rapidly changing environment, excessive and rapid regulation carries the risk of undesirable outcomes in a way that does

---

\* Željko Jović is at National bank of Serbia, Belgrade; Kralja Petra 12. E-mail: [zeljko.jovic@nbs.rs](mailto:zeljko.jovic@nbs.rs)

\*\* Ivan Nikolić is at Economics Institute, Belgrade; Kralja Milana 16. E-mail: [ivan.nikolic@ecinst.org.rs](mailto:ivan.nikolic@ecinst.org.rs)

not exploit the full potential of innovative technologies. The development and increasing use of financial technologies affects the activities of all participants in the financial market, which imposes the need for continuous learning and adaptation of users and providers of these services, as well as supervisors and regulators. An additional challenge for financial institutions is the fact that competition in the provision of financial services comes from IT companies, which necessarily imposes the need to adapt its business models. Financial institutions are facing one of the biggest business challenges. All this brings special challenges for the creators of regulatory standards (RegTech) and the development of supervision based on new technologies (SupTech).

**Keywords:** FinTech, Risks; RegTech; SupTech

**JEL Classification:** G20, G21, G32, E58

## Introduction

Technology and innovation are transforming the global financial landscape, presenting opportunities, risks and challenges for regulated institutions and authorities alike. One important area of innovation is the application of financial technology (FinTech) for regulatory and compliance requirements and reporting by regulated institutions (RegTech), and applications of FinTech used by authorities for regulatory, supervisory and oversight purposes (SupTech) (Financial Stability Board (FSB), 2020). This paper examines the financial innovations, bearing in mind variety of new and existing risks that come with digital technologies.

FinTech innovations are affecting many different areas of financial services, such as FinTech credit, digital currencies, distributed ledger technology, artificial intelligence and machine learning. Development of financial services could contribute to macroeconomic stability by lowering constraints, resulting in faster economic growth, less poverty and lower income inequality but it also could be a source of instability (Weller and Zulfigar, 2013).

Aside from that, important innovation is application of new technologies to help authorities to improve their supervisory capabilities (known as SupTech) and by institutions to meet their regulatory requirements (known as RegTech). FinTech, RegTech and SupTech are strategic concepts in the financial sector and connected in many ways, however each one needs different perspectives and approaches to produce sound policies. They all share “technology”, but technological tools are used for various purposes in each area (Zeranski and Sancak, 2020).

Financial stability could benefit from SupTech and RegTech tools, whereas regulated institutions could improve compliance outcomes, enhance risk management capabilities, and generate new insights into the business for improved decision-making

by using RegTech (FSB, 2020). The opportunities offered by SupTech and RegTech have been created by a combination of factors that include the substantial increase in availability and granularity of data, and new infrastructure such as cloud computing and application programming interfaces (APIs) which allow large data sets to be collected, stored and analysed more efficiently (FSB, 2020).

After the global financial crisis, innovations made possible by digital technologies led many to claim, that once again banks were on the verge of extinction and about to be replaced or fundamentally disrupted by FinTech firms (Stulz, 2019).

Additionally, FSB stress that crypto-assets markets are fast evolving and could reach a point where they represent a threat to global financial stability due to their scale, structural vulnerabilities and increasing interconnectedness with the traditional financial system. The FSB has done report on COVID-19 pandemic and implications for financial stability, in which they elaborated how the COVID-19 pandemic accelerated the trend toward digitalisation of retail financial services. Said report stressed the importance of digital innovation to improve market access, the range of product offerings and convenience in the last two years (2020-21).

BigTech firms made rapid revenue growth during the pandemic, due to the changed way of life during lockdowns and dependency to online platforms (Nikolic and Filipovic, 2021). Therefore, the prompt change of work and learning in 2020 stressed the importance of cloud computing platforms, which saw strong growth. Particularly BigTechs, larger FinTechs and incumbent financial institutions that were agile and able to invest in digital technologies seem to have gained market share in retail financial services. Incumbent financial institutions that were unable to keep up with these developments and provide their customers with the online services they demanded seem to have lost market share. While available proxies do not yet show a broad-based increase in market concentration, BigTechs do tend to dominate specific markets (e.g. cloud services, mobile payments in some EMDEs).

## **FinTech**

The term FinTech (sometimes: Fintech, Fin-tech, or FinTech) is a neologism which originates from the words “financial” and “technology” and describes in general the connection of modern and, mainly, Internet-related technologies (e.g., cloud computing, mobile Internet) with established business activities of the financial services industry (e.g., money lending, transaction banking) (Gomber et al., 2017). The Financial Stability Board (FSB) defines FinTech as technologically enabled innovation in financial services that could result in new business models, applications, processes or products with an associated material effect on financial markets and institutions and the provision of financial services.

FinTech could affect market structure through channels such as FinTech credits, BigTech companies and third parties' services (Vučinić, 2020). FinTech credits provide alternative sources of funding where borrowers communicate directly to lenders. BigTech companies have already confirmed themselves in the world of internet technology which makes it easier for them to expand further to other fields such as financial service thus becoming strong competitors to other FinTech companies. According to the words of Tao Zhang (2019), the IMF Deputy Managing Director, FinTech is expected to promote competition in the financial sector primarily in the aspects of payments clearing and settlement, and to increase financial inclusion.

FinTech will bring both opportunities and risks to financial stability that policy-makers, regulators, supervisors and overseers should consider. Thus, it is important to highlight that there may be overlaps and trade-offs between financial stability concerns and other regulatory lenses.

There are variety of benefits, which include:

- decentralisation and increased intermediation by non-financial entities;
- greater efficiency, transparency, competition and resilience of the financial system;
- and greater financial inclusion and economic growth, particularly in emerging market and developing economies.

Potential risks in FinTech are:

- microfinancial risks, made by individual firms, financial market infrastructures (FMIs) or sectors particularly vulnerable to shocks (e.g. credit risk, leverage, liquidity risk, maturity mismatch and operational risks, especially cyber and legal);
- macrofinancial risks, system-wide vulnerabilities that can amplify shocks to the financial system and thereby raise the likelihood of financial instability (e.g. non-sustainable credit growth, increased interconnectedness or correlation, incentives for greater risk-taking by incumbent institutions, procyclicality, contagion and systemic importance) (FSB, 2017).

FinTech expansion raises a need for stronger international cooperation especially in terms of cyber security, anti-money laundering and combating of financing terrorism, the development of regulatory and supervisory frameworks, payment and securities settlement systems and cross-border payments. In other words, in an increasingly interconnected global financial marketplace, there is a broader and faster propagation of risk, requiring supervisors to have the tools to keep pace (Soramäki and Straley, 2019). Therefore, FSB, BIS, IMF, WB, IOSCO, and other multinational or international organizations have new responsibilities and new roles. A successful financial supervisory system reform increases the value of supervisory activities and services.

While many FinTech activities are covered within existing regulatory frameworks, the FSB stocktake of regulatory approaches to FinTech finds that majority of jurisdictions surveyed have already taken or plan to take regulatory measures to

respond to FinTech. The scope and scale of changes or planned changes vary substantially, depending, among other things, on the relevant size and structure of domestic financial and FinTech sectors – and the flexibility provided already by the existing regulatory framework. Some regulatory authorities have recently issued publications or proposals on aspects of FinTech. Several jurisdictions have introduced regulatory sandboxes, hubs or accelerators in order to promote innovation and improve interactions with new FinTech firms. In general, the policy objectives pursued are mostly consumer and investor protection, market integrity, financial inclusion and promoting innovation or competition (FSB, 2017).

### *Regulatory and Industry Sandboxes*

A regulatory sandbox usually refers to live testing of new products or services in a controlled environment (BIS, 2018). The sandbox creates an environment for businesses to test products with less risk of being “punished” by the regulator (Zetzsche et al., 2017). On the other hand, regulatory sandboxes give regulators an opportunity to learn the risks associated with new technologies and right-size regulation accordingly (Menon, 2017). They set bridges between financial services providers and supervisors and create a technological communication environment, which has been a problematic area for both sides.

Regulatory sandboxes have a revolutionary capacity in the regulatory and supervisory landscapes both for industry members and supervisors. However, regulatory sandboxes may hold both benefits and risks (De Koker et al, 2020).

### *Innovation Hubs*

An innovation hub is an innovation facilitator set up by supervisory agencies that provides support, advice, or guidance to regulated or unregulated firms in navigating the regulatory framework or identifying supervisory policy or legal issues and concerns (BIS, 2018). They focus on developing innovative products, services, and training in a specific area of their innovation community, taking targeted actions to help overcome key challenges in that field (EIT, 2020).

An innovation hub can be described as an information exchange regime on FinTech matters (BIS, 2018). Even though innovation hubs are considered for companies that have a new business model or technology, these platforms may help supervisors capture market trends and potential developments and directions. Therefore, an innovation hub is somehow the source and centre of information for proactive and predictive supervision.

Many authorities have already implemented innovation facilitators, such as regulatory sandboxes, innovation hubs, and innovation accelerators, or other forms of

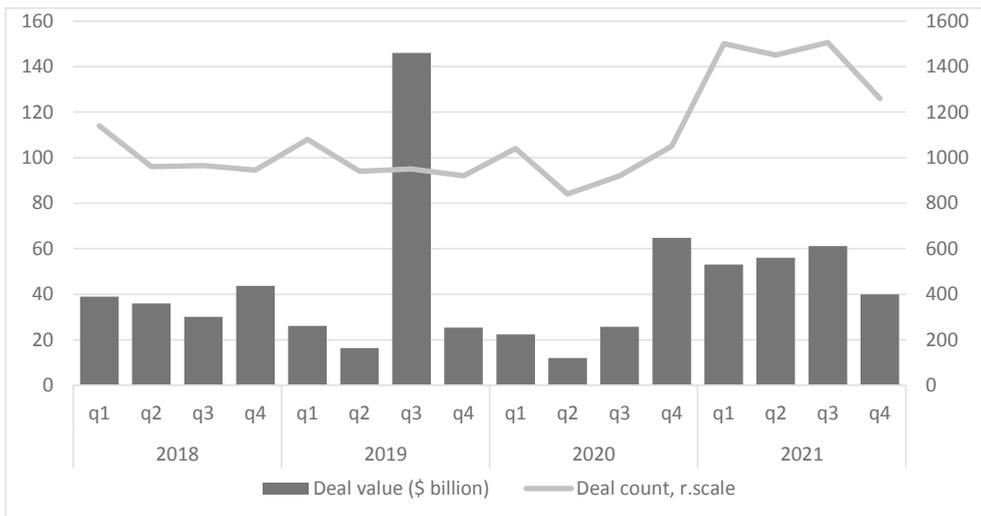
interaction such as workshops, conferences, and regular dialogue with market participants (FSB, June 2017).

The surveys done in 2019 by UNSGSA and both IMF and World Bank show 4 types of innovative regulatory initiatives which are innovation office, regulatory sandbox, RegTech and special contact for Fintech questions, implemented in 30 European countries. Majority of countries implemented innovation offices (77%) and special contact for FinTech questions (61%), whereas regulatory sandboxes and RegTech are implemented by less than 30% of said countries.

### *FinTech analysis*

KPMG made an overview of the FinTech landscape through analyses of global and regional FinTech investments, and key trends are developments within FinTech and financial services. Figure 1 display total global investment activity in FinTech in 2018-2021, which continues to evolve.

Figure 1: Total global investment activity in FinTech



Source: Pulse of Fintech H2'21, Global Analysis of Investment in Fintech, KPMG International

In the first nine months of 2016, global investment in FinTech reached \$21 billion, marking a five-fold increase over 2013. Using the data from KPMG's analysis for interval of four years (2018–2021), the biggest investment was made in the third quarter of 2019, with the value of \$146 billion, as seen in the Figure 1.

With FinTech, users can connect through a variety of mobile services, such as making payments, transferring money, requesting loans, buying insurance, managing

assets, and making investments among others (Ryu, 2018). Some FinTech applications may suggest cheaper transaction costs for users, compared with traditional financial service providers, directly supplying standardized services through a mobile services platform without intermediation (Mackenzie, 2015). Seamless transactions refer to the benefits related to transactions using a FinTech that eliminates traditional financial institutions, enabling users to manage transactions on economic platforms, resulting in simpler and quicker financial operations (Chishti, 2016; Zavolokina et al., 2016). Moreover, non-financial providers (that is, IT companies) may create and offer innovative, user-friendly financial products and services to customers, as they supply their products and services directly (Mascarenhas et al, 2021).

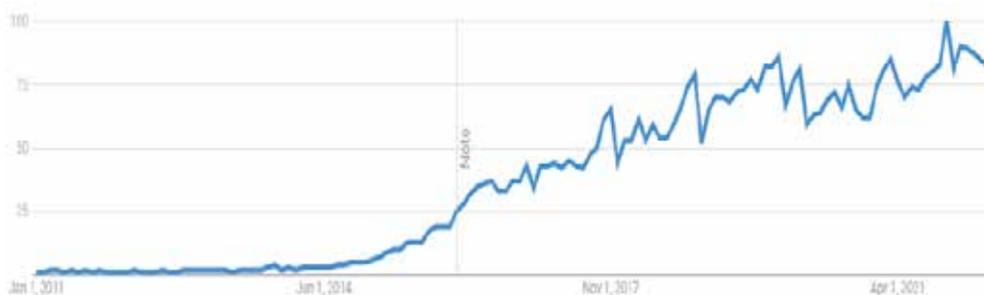
### *Relationship between banks, FinTech and BigTech*

Rene Stulz (2019) explained the regulations differences between banks and FinTech versus BigTech. BigTech firms are technology companies with established presence in the market for digital services (Frost et al., 2019). They are firms that have successful digital platforms, such as Amazon, Facebook, Google Alibaba and Tencent. The Chinese counterparts of the U.S. firms have already made big inroads in financial services markets—but the U.S. firms have not. The challenges for banks posed by the entry of BigTech into finance are quite different from the challenges posed by FinTech firms. The typical FinTech firm is a specialized firm that challenges a specific product line of banks. For instance, a credit FinTech firm aims to seize market share from banks, typically in a specialized segment of the credit market. On contrary, BigTech firms have the ability to challenge banks across numerous product lines as they can lead a frontal assault as opposed to attacking niches.

### *Trends*

According to P. Schueffel and Google in 2016, the term FinTech received monthly on average approximately 201.000 google searches worldwide. When normalizing the scale between the fewest search entries and the most search request over the past five years on a scale between 0 and 100, a significant increase can be seen in the interest of the term Fintech. The Picture 1 shows the trend for period 2011-2022.

Figure 2: Trend of the word “FinTech” for the period 2011-2022



Source: Google Trends, <https://trends.google.com/trends/explore?date=2011-11-01%202022-05-17&q=fintech>

The highest interest was in October 2021 and that the curve grew rapidly in the last five years.

KPMG made a report of an overview of the FinTech landscape through analyses of global and regional FinTech investments and key trends and developments within FinTech and financial services, and it shows top 10 global FinTech deals in 2021, shown in Table 2.

Table 2: Top 10 global fintech deals in 2021

Name	Value	Place	Type
1. Refinitiv	\$14,8B	London, UK	Institutional/B2B - M&A
2. Nets	\$9,2B	Ballerup, Denmark	Payments - M&A
3. Adenza	\$3,75B	San Francisco, US	Institutional/B2B - Buyout
4. Robinhood	\$3,4B	Menlo Park, US	Wealth/Investment management - Series G
5. Verafin	\$2,75B	St.John's, Canada	Institutional/B2B - M&A
6. Paidy	\$2,78B	Tokyo, Japan	Lending - M&A
7. Itiviti Group	\$2,6B	Stockholm, Sweden	Institutional/B2B - M&A
8. SoFi	\$2,4B	San Francisco, US	Lending - Reverse merger
9. Divvy	\$2,3B	Draper, US	Payments/transactions - M&A
10. Tink	\$2,2B	Stockholm, Sweden	Banking - M&A

Source: Pulse of FinTech H2'21, <https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/02/pulse-of-fintech-h2-21.pdf>

Said report stress the interest in cyber security in previous year, driven by disruptions that gained international attention, including major ransomware attacks and the use of exploitable malware on non-traditional IT infrastructure.

KPMG's top FinTech trends for 2022 include following predictions:

- growing number of banks will offer embedded solutions;
- FinTechs will focus on branding themselves as data organizations;
- stronger focus on dealmaking in underdeveloped regions;
- increased regulatory scrutiny of embedded finance offerings.

## RegTech

The FSB defines RegTech as any range of applications of FinTech for regulatory and compliance requirements and reporting by regulated financial institutions. This can also refer to firms that offer such applications. Therefore, RegTech is often regarded as a subset of FinTech that focuses on facilitating regulatory compliance more efficiently and effectively than existing capabilities. There is also a close link with SupTech or the use of FinTech by supervisory authorities (Jovic, 2019). FinTech refers to the use of technology to deliver financial solutions, and RegTech describes the use of technology in the context of regulatory monitoring, reporting, and compliance (Arner et al., 2019). The UK's Financial Conduct Authority defines RegTech as a subset of FinTech which focuses on technologies that may facilitate the delivery of regulatory requirements more efficiently and effectively than existing capabilities (FCA, 2016). Contrary to the FCA's definition, Arner et al. (2017) argue that RegTech cannot be simplified as a category of FinTech. RegTech and FinTech may share or use similar or the same technology, but one is not the subset of the other one. The same situation also holds for SupTech. Both SupTech and RegTech support the fulfilment of such financial system goals as stability, integrity, and consumer protection (Perlman et al., 2020).

At the moment, the widespread adoption of RegTech/SupTech solutions certainly seems to reduce certain risks, like the use of machine learning tools to monitor potential market abuse practices probably has the potential to improve market integrity. Authorities such as the ECB and the U.S. Fed are using Natural Language Processing (a form of AI) to help them identify financial stability risks (Gasparrri, 2019).

A number of supply-based developments and demand-based needs are combining to potentially transform the way financial institutions comply with regulation and supervisory authorities oversee market participants.

The use of technology for compliance and supervisory monitoring predates the financial crisis of 2007. However, a new regulatory landscape in response to the crisis has been a catalyst for greater use of technology. Foremost among the technological drivers are the widespread use of cloud computing, the increased acceptance of Application Programming Interfaces (APIs) and advances in the fields of Artificial Intelligence and Machine Learning (AI/ML). Cloud computing allows for the use of an online network of hosting processors, increasing the scale and flexibility of computing capacity. APIs comprise rules and an interface for communication and interaction between different software programmes. AI is the theory and development of computer systems able to perform tasks that traditionally require human intelligence, whereas ML, a form of AI, is a method of designing a sequence of actions to solve a problem that optimise automatically through experience and with limited or no human intervention (Armstrong, 2018). Regulatory pressure and budget limitations are pushing the market towards an increased use of automated software to replace human decision-making activities. AI/ML tools are often used to implement such

automation, with the calibration of the tools based on the recognition of patterns and relationships in large amounts of structured or unstructured data, also known as Big Data (Armstrong, 2018).

## SupTech

Supervisory technology (SupTech) is a set of technological tools and solutions for supervisory agencies to carry out their responsibilities in the FinTech world (Zeranki and Sancak, 2020). Thus, strong supervisory policies increase market integrity and decrease financial crisis risk. Supervisory programs have implications on the investment environment, and therefore, SupTech has crucial importance for an economy.

In a sense, SupTech is the name of FinTech when it is used for supervisory purposes. FinTech, RegTech and SupTech operators may utilize the same technological tools such as AI/ML, NLP, cloud computing, DLT, and others in their interests and purposes. When it is used within the context of a regulator's function, RegTech may have a similar meaning to SupTech. However, when used within the context of financial services provider's function, it has a different status. Furthermore, SupTech has a focus on supporting supervisory authorities in their assessment of compliance works, not on assisting compliance with laws and regulations (BIS, 2018).

The paper of Castri et al. (2019) defines SupTech as “the use of innovative technology by financial authorities to support their work” in their paper's context. According to the authors, the term “innovative technology” refers to the application of big data or artificial intelligence (AI), the tools that financial authorities use, whereas “financial authorities” refers to both supervisory and non-supervisory authorities except the authorities in charge of monetary and macroeconomic policies (Castri et al., 2019).

Despite SupTech system has not been directly named, the main features have been outlined by the Basel Committee on Banking Supervision of the BIS: “The supervisor uses an appropriate range of techniques and tools to implement the supervisory approach and deploys supervisory resources on a proportionate basis, taking into account the risk profile and systemic importance of banks” (BIS, 2012).

The FSB defines SupTech (FSB, November 2017) in the glossary as “Applications of FinTech by supervisory authorities”. The FSB has also described SupTech within the same report: “SupTech is the use of these technologies by public sector regulators and supervisors.” The term “technologies” refers to artificial intelligence (AI) and machine learning (ML).

Both the BIS and the FSB's definitions mainly capture the concept. However, there is no universally agreed SupTech definition, and variations exist based on the applications (Boeddu et al., 2018).

To ensure that people benefit from digital financial services, governments need to ensure that appropriate regulations and consumer protection safeguards are in place

(Demirgüç-Kunt et al., 2018). Therefore, SupTech is a set of safeguards. FinTech and SupTech must at least develop parallelly, in order to protect financial system and financial consumers against FinTech related risks and threats. If not, a FinTech dominant financial sector without SupTech might be huge risk for economy. On the other hand, SupTech dominant sector may induce the financial industry to become more technology-oriented, and it is a driver for advancement and development of financial stability (Zeranki and Sancak, 2020).

Zeranki and Sancak stress that SupTech refers to the crossroads of technology and supervision, and it is, in a sense, a strategic risk management system in the FinTech world, and it is critical that a “SupTech system” and a “supervisory system” are distinguished from each other: A SupTech system is mainly a component of a supervisory system, but each has a different meaning. Thus, the definition of SupTech should be neither restricted to the pure governmental landscape nor financial authorities and it should not be framed with some specific technology tools, such as AI, ML, or NLP. As more technological tools become available, supervisors can get the benefit of them to carry out their responsibilities.

## Risks

Cyber incidents remain a threat to the financial system and are rapidly growing in frequency and sophistication. In light of increasing financial stability concerns, especially given the digitalisation of financial services and increased use of third-party service providers, the Financial Stability Board (FSB, 2021) explored whether harmonisation in cyber incident reporting could be achieved.

The FSB found that fragmentation exists across sectors and jurisdictions in the scope of what should be reported for a cyber incident, methodologies to measure severity and impact of an incident, timeframes for reporting said incidents and how cyber incident information is used. This subjects financial institutions that operate across borders or sectors to multiple reporting requirements for one cyber incident. At the same time, financial authorities receive heterogeneous information for a given incident, which could undermine a financial institution’s response and recovery actions. This underscores a need to address constraints in information-sharing among financial authorities and financial institutions.

Thus, FSB has identified three ways to achieve greater convergence in cyber incident reporting:

- *Develop best practices.* Identify a minimum set of types of information authorities may require related to cyber incidents to fulfil a common objective (e.g. financial stability, risk assessment, risk monitoring) that authorities could consider when developing their cyber incident reporting regime.

- *Identify common types of information to be shared.* Identify key information items that should be shared across sectors and jurisdictions, and to understand any legal and operational impediments to sharing such information.
- *Create common terminologies for cyber incident reporting.* Harmonised cyber incident reporting schemes necessitate a ‘common language’. In particular, a common definition for ‘cyber incident’ is needed that avoids the reporting of incidents that are not significant for a financial institution or financial stability.

FSB (2017) identified ten potential areas where international bodies and national authorities should draw attention regarding FinTech when performing regular risk assessment and development of micro and macroprudential regulatory frameworks, whereas the first three of them are distinguished as priority areas.

1. *Managing operational risks from third-party service providers.* Authorities should determine if current oversight frameworks for important third-party service providers to financial institutions are appropriate, e.g. in cloud computing and data services, especially if financial institutions rely on the same third-party service providers.
2. *Mitigating cyber risk.* Recent reports of significant and successful cyber attacks underscore the difficulties of mitigating cyber risk. Ex ante contingency plans for cyber attacks, information sharing, monitoring, a focus on incorporating cyber security in the early design of systems, and financial and technology literacy could help to lower the probability of cyber events that have adverse effects on financial stability.
3. *Macrofinancial risks monitoring.* While there are currently no compelling signs of these risks materialising, experience shows that they can emerge quickly if left unchecked. Systemic importance and procyclicality could emerge from several sources, including from greater concentration in some market segments and if funding flows on FinTech lending platforms were to become large and unstable. Any assessment of the implications of FinTech for financial stability is challenged by the limited availability of both official and privately disclosed data in the FinTech area. Thus, authorities should consider developing their own capacity to access existing and new sources of information.
4. *Cross-border legal issues and regulatory arrangements.* Innovations in cross-border lending, trading and payment transactions, including via smart contracts, raise questions about the cross-jurisdictional compatibility of national legal frameworks, given the fact that the legal validity and enforceability of smart contracts and other applications of distributed ledger technology (DLT) are in some cases uncertain and should be discussed further.
5. *Governance and disclosure frameworks for big data analytics.* Big data analytics are driving transformation across industries with the ability to conduct extensive analytics rapidly and enhance risk identification and assessment. The complexity and opacity of some big data analytics models makes it difficult for

- authorities to assess the robustness of the models or new unforeseen risks in market behaviour, and to determine whether market participants are fully in control of their systems.
6. *Assessing the regulatory perimeter and updating it on a timely basis.* Regulators should be agile when there is a need to respond to fast changes in the FinTech space, and to implement or contribute to a process to review the regulatory perimeter regularly.
  7. *Shared learning with a diverse set of private sector parties.* In order to support the benefits of innovation through shared learning and through greater access to information on developments, authorities should continue to improve communication channels with the private sector and to share their experiences with regulatory sandboxes, accelerators and innovation hubs, as well as other forms of interaction.
  8. *Further developing open lines of communication across relevant authorities.* Due to the potentially growing importance of FinTech activities and the interconnections across the financial system, authorities may wish to develop further their lines of communication to ensure preparedness.
  9. *Building staff capacity in new areas of required expertise.* Supervisors and regulators should consider placing greater emphasis on ensuring they have the adequate resources and skill-sets to deal with FinTech.
  10. *Studying alternative configurations of digital currencies.* The implications of alternative configurations of digital currencies for national financial systems, and the global monetary framework should be studied, as well as the potential implications of digital currencies for monetary policy, financial stability and the global monetary system (Nikolić, 2019). One issue is the use of some virtual currencies for illegal activities (including cyber attacks).

To draw out the supervisory and regulatory issues of FinTech, the FSB (2017) developed a framework that defines the scope of FinTech activities and identifies the potential benefits and risks to financial stability. It provides a basis on which future analysis and monitoring can be made. Given the fact that most FinTech activities are currently small compared to the overall financial system, the analysis focuses on conceivable benefits and risks. Nonetheless, international bodies and national authorities should consider taking FinTech into account in their existing risk assessments and regulatory frameworks in light of its rapid evolution.

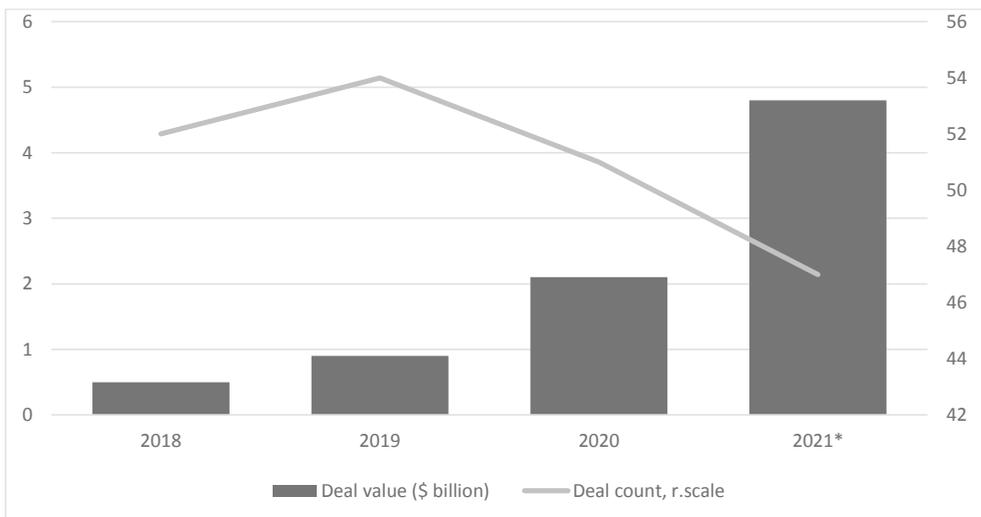
Increased cooperation will be of great importance to mitigate the risk of fragmentation or divergence in regulatory frameworks, which could impede the development and diffusion of beneficial innovations in financial services and therefore limit the effectiveness of efforts to promote financial stability.

The increased use of technology and digitisation, propelled by the rapid move to work-from-home arrangements due to the COVID-19 pandemic, opened up new possibilities for cyber attacks, as explained in FSB Annual Report (2021).

Efficient and effective response to and recovery from a cyber incident is essential to limiting any related financial stability risks. The number of cyber attacks has increased significantly, especially since the pandemic, thus financial institutions need to consider enhancements to their cyber risk management processes, cyber incident reporting, response and recovery activities, as well as management of critical third-party service providers (e.g. cloud services).

KPMG made a report of an overview of the FinTech landscape through analyses of global and regional FinTech investments and key trends and developments within FinTech and financial services for period 2018-2021, in which they stress the interest in cyber security in previous year, driven by disruptions that gained international attention, including major ransomware attacks and the use of exploitable malware on non-traditional IT infrastructure. Between 2020 and 2021, investment in cyber security more than doubled, although the \$2.7 billion acquisition of Canadian fraud detection platform Verafin accounted for more than half of this total. That report saw a combination of M&A and VC investment in the space, including a \$310 million raise by US-based Fireblocks, the \$250 million merger between Switzerland-based zero knowledge rollup blockchain company Hermez and India-based crypto company Polygon, and the acquisition of Israel-based cyber security firm GK8 by Celsius Network.

Figure 3: Total global investment activity (VC, PE and M&A) in FinTech: cyber security



Source: Pulse of FinTech H2'21, <https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/02/pulse-of-fintech-h2-21.pdf>

Fraud prevention continued to be a major priority for organizations across jurisdictions in 2021, evidenced by the acquisition of above mentioned Canadian fraud

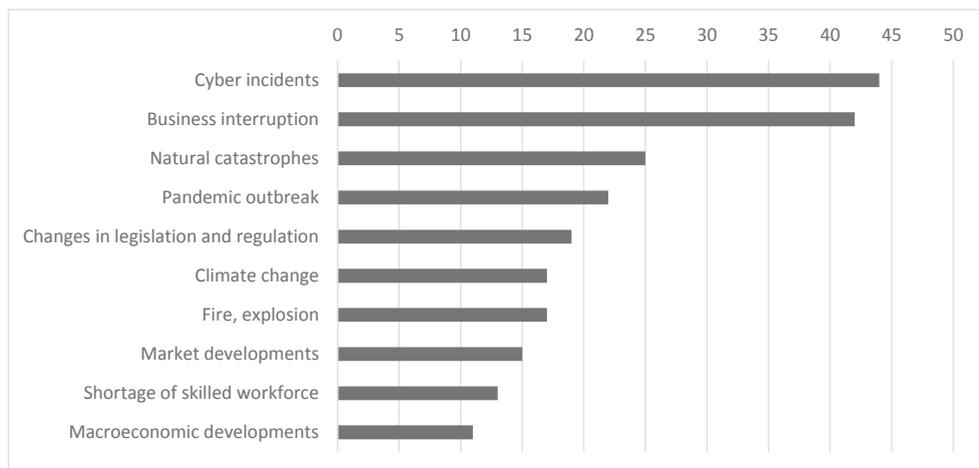
detection platform Verafin by Nasdaq in 2021. Investors and corporates showed particular interest in proactive and pre-emptive security solutions, such as solutions aimed at connecting known cyber indicators of compromise with different types of fraud and solutions that use behavioural analytics to understand potential fraudulent behaviours.

As a result of the significant increase in cloud-based activities and digital transactions and the increasing bombardment of companies by malicious attackers over the last two years, interest in managed detection and response (MDR) and endpoint detection and response (EDR) using AI, automation and robotics solutions has grown significantly. Over the next year, this will likely lead investors to focus on security platforms able to manage the complex array of security needs of companies. There will likely also be more M&A activity as platform providers acquire bolt-on solutions to extend their value.

The reality is that cyber attacks are evolving as quickly as innovative technologies and processes, presenting enormous risk to organizations who might not be able to recover from a major attack. In 2021, as companies accelerated their activities in the cloud and the speed of their digital transformation efforts, they increasingly recognized the importance of secure DevOps. They also increased their investments in related areas, including cyber resilience, breach remediation, vulnerabilities testing, and ensuring basic security hygiene to ensure rapid change doesn't leave risk exposure.

Artificial Intelligence (AI) is creating a rush of opportunities in the financial sector, but financial organizations need to be aware of the risks inherent in the use of this technology (Ashta and Herrmann, 2021). Financial organizations are integrating AI in their operations: in-house, outsourced, or ecosystem-based. The growth of AI-based FinTech firms has encouraged several mergers and acquisitions among financial service providers and wealth managers as they grapple with volatility, uncertainty, complexity, and ambiguity. AI's unique promise of combined cost reduction and increased differentiation makes it generally attractive across the board. However, perhaps other than fraud detection, these benefits depend on the scale of an organization. Risk arises from nonrepresentative data, bias inherent in representative data, choice of algorithms, and human decisions, based on their AI interpretations (and whether humans are involved at all once AI has been unleashed). Risk reduction requires a vigilant division of labour between AI and humans for the foreseeable future.

Figure 4: The most important global business risks for 2022 (in %)



Source: <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html> Note: The Allianz risk barometer shows that the highest ranked risk are cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties).

A combination of technological innovations, including AI, is changing business as it responds to volatility, uncertainty, complexity and ambiguity in the financial sector, popularized in the literature as a VUCA world (Millar et al., 2018).

The Allianz risk barometer, shown in Figure 4, represents the most important global business risks for 2022, with cyber incidents (e.g. cyber crime, IT failure/outage, data breaches, fines and penalties) ranked in first place.

## Conclusion

The emergence of innovative business models and the rise of new competitors have a tremendous influence on current industry dynamics, although the financial industry has been traditionally an early adopter and intensive user of new developments in information and communication technologies.

Rapid developments of FinTech and COVID-19 pandemic influenced financial markets and business models of traditional financial institutions. Significant entry of BigTech companies to the world of financial services could make strong implications and potentially threaten activities of traditional financial services providers, given the fact that BigTechs are relatively easily entering the new markets due to their strong technological developments and big data access.

Despite variety of opportunities and benefits that FinTech brings to market players and customers, at the same time it has numerous potential risks, as it poses threats to financial stability in terms of micro and macroeconomic risks. Thus, international institutions such as the FSB, IMF and WB are calling for international cooperation among national and international institutions with the aim to address and reduce regulatory gaps, prevent occurrence of potential risks and mitigate the likelihood the risks develop posing systemic risks which could further jeopardize financial stability on local levels and potentially spread to the global level.

SupTech system is mainly a component of a supervisory system, whereas a full-fledged supervisory system should include:

- a well-organized financial system,
- a well-functioning SupTech system,
- SupTech oriented financial infrastructure,
- dematerialized financial instruments,
- a supervisory model in line with the FinTech nature,
- in-house digitalization,
- real-time data, automated data collection, and data analytics tools,
- experienced and dedicated supervisory personnel and IT staff,
- prudential supervisory disclosure policy,
- as well as other features that help supervisors carry out their responsibilities efficiently and effectively.

Large cyber attacks pose a real threat to financial stability as they are becoming ubiquitous, sophisticated and destructive, and the interconnected world is open to cyber security failures and cyber crime. Therefore, it stresses the importance of setting up and continual development of a culture of cyber security. In spite of numerous benefits of AI/ML, including increased financial inclusion through providing convenient and efficient digital financial services, it has potential for cyber threats and attacks. Rapid FinTech development and risks from cyber crime and cyber attacks will continue to accelerate parallelly, and thus it will require more supervision from regulators, preventive actions and risk-based thinking.

The COVID-19 pandemic has had a significant impact on market structure in retail financial services. Despite scarce comprehensive data on market shares in retail financial services, available proxies and insights from market participants suggest that BigTechs in particular have further expanded their footprint in financial services. Likewise, larger FinTechs and incumbent financial institutions have also benefited, as they have been able to use their investments in digital technologies and their large client bases to further build out market shares, whereas smaller FinTechs and digital laggards appear to have benefited to a lesser degree and may struggle to compete going forward. The trend toward greater use of digital financial services may bring many benefits for efficiency, financial inclusion and diversity of the financial sector.

Expansion of BigTech and FinTech firms into financial services can bring benefits such as improved cost efficiencies and wider financial inclusion for previously underserved groups, with the potential for market dominance. However, there could be negative financial stability implications from dependence on a limited number of BigTech and FinTech providers in some markets, the complexity and opacity of their partnership activities, and potential incentives for risk taking by incumbent financial institutions to preserve profitability. Consumer protection risks could arise from greater dependency on technology and potential data protection issues. Thus, authorities have taken a range of policy actions during the pandemic that may impact market structure and the role of FinTech, BigTech and incumbent financial institutions. These actions relate to financial stability, competition, data privacy and governance issues.

The cooperation between regulatory and supervisory authorities, including those charged with overseeing the bank and non-bank sectors, and where relevant, with competition and data protection authorities, is of great importance.

## REFERENCES

- Allianz Risk Barometer, (January 2022). Available at: <https://www.agcs.allianz.com/news-and-insights/reports/allianz-risk-barometer.html>
- Armstrong, P. (2018). *Developments in RegTech and SupTech*. Paris: Paris Dauphine University. Available at: [https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070\\_speech\\_on\\_regtech.pdf](https://www.esma.europa.eu/sites/default/files/library/esma71-99-1070_speech_on_regtech.pdf)
- Ashta, A., & Herrmann, H. (2021). Artificial intelligence and fintech: An overview of opportunities and risks for banking, investments, and microfinance. *Strategic Change*, 30(3), 211-222. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1002/jsc.2404>
- Assessment of Risks to Financial Stability from Crypto-assets (February 16, 2022). Financial Stability Board, Available at FSB: <https://www.fsb.org/2022/02/assessment-of-risks-to-financial-stability-from-crypto-assets/>
- Berg, G., Guadamillas, M., Natarajan, H., & Sarkar, A. (2020). *Fintech in Europe and Central Asia*. Available at: <https://openknowledge.worldbank.org/handle/10986/33591>
- Chishti, S. (2016). How peer to peer lending and crowdfunding drive the fintech revolution in the UK. In *Banking beyond banks and money* (pp. 55-68). Springer, Cham.
- Cyber Incident Reporting: Existing Approaches and Next Steps for Broader Convergence. (October 19, 2021). Financial Stability Board, Available at FSB: <https://www.fsb.org/2021/10/cyber-incident-reporting-existing-approaches-and-next-steps-for-broader-convergence/>
- Financial Stability Implications from FinTech, Supervisory and Regulatory Issues that Merit Authorities' Attention. (June 27, 2017). Financial Stability Board, Available at FSB: <https://www.fsb.org/2017/06/financial-stability-implications-from-fintech/>
- FinTech and Market Structure in the COVID-19 Pandemic, Implications for financial stability. (March 21, 2022). Financial Stability Board, Available at FSB: <https://www.fsb.org/2022/03/fintech-and-market-structure-in-the-covid-19-pandemic-implications-for-financial-stability/>
- Frost, J., Gambacorta, L., Huang, Y., Shin, H. S., & Zbinden, P. (2019). BigTech and the changing structure of financial intermediation. *Economic Policy*, 34(100), 761-799.
- FSB Press release. FSB report highlights increased use of RegTech and SupTech. (October 9, 2020). Available at FSB: <https://www.fsb.org/wp-content/uploads/R091020-1.pdf>

- Gasparri, G. (2019). Risks and opportunities of RegTech and SupTech developments. *Frontiers in Artificial Intelligence*, 14. Available at: <https://www.frontiersin.org/articles/10.3389/frai.2019.00014/full>
- Gomber, P., Koch, J. A., & Siering, M. (2017). Digital Finance and FinTech: current research and future research directions. *Journal of Business Economics*, 87(5), 537-580. Available at: <https://link.springer.com/article/10.1007/s11573-017-0852-x>
- Jakšič, M., & Marinč, M. (2019). Relationship banking and information technology: The role of artificial intelligence and FinTech. *Risk Management*, 21(1), 1-18. Available at: <https://link.springer.com/article/10.1057/s41283-018-0039-y>
- Jovic, Z. (2019). Insurance Supervision On the Threshold Of the Fourth Industrial Revolution with Special Emphasis on the Significance of Actuarial Models. In: *Contemporary Trends In Insurance At The Beginning Of The Fourth Industrial Revolution*, (eds) Jelena Kočović, Milo Tomašević, Biljana Jovanović Gavrilović, Branislav Boričić, Evica Petrović, Marija Koprivica: Faculty of Economics.
- KPMG. (January, 2022). Pulse of Fintech H2'21. Available at: <https://assets.kpmg/content/dam/kpmg/xx/pdf/2022/02/pulse-of-fintech-h2-21.pdf>
- Mackenzie, A. (2015). The fintech revolution. *London Business School Review*, 26(3), 50-53.
- Mascarenhas, A. B., Perpétuo, C. K., Barrote, E. B., & Perides, M. P. (2021). The influence of perceptions of risks and benefits on the continuity of use of fintech services. *BBR. Brazilian Business Review*, 18, 1-21.
- Menon, R. (2017). Financial Regulation-the Forward Agenda. In *Keynote Address by Managing Director, Monetary Authority of Singapore, at the Australian Securities and Investments Commission (ASIC) Annual Forum (Vol. 20)*.
- Nikolić, I & Filipović, S. (2021). Comparative Analysis of the Economic Policy Response to Covid-19 in the EU-27 and Republic of Serbia, *Ekonomika preduzeća*, 2021, vol. 69, n. 7-8, p. 460-475, DOI: 10.5937/EKOPRE2108460N
- Nikolić, I. (2019). Spillover effects of non-standard monetary policy measures and of future monetary policy normalisation on Serbia, *Bančni vestnik, The journal for Money and Banking*, ISSN 0005-4631, Ljubljana, Vol. 68, n.11, november 2019
- Promoting Global Financial Stability, 2021 FSB Annual Report. (October 27, 2021). Financial Stability Board, Available at FSB: <https://www.fsb.org/wp-content/uploads/P271021.pdf>
- Schueffel, P. (2016). Taming the beast: A scientific definition of fintech. *Journal of Innovation Management*, 4(4), 32-54. Available at: [https://journalsojs3.fe.up.pt/index.php/jim/article/view/2183-0606\\_004.004\\_0004](https://journalsojs3.fe.up.pt/index.php/jim/article/view/2183-0606_004.004_0004)
- Stulz, R. M. (2019). FinTech, BigTech, and the future of banks. *Journal of Applied Corporate Finance*, 31(4), 86-97. Available at: <https://onlinelibrary.wiley.com/doi/abs/10.1111/jacf.12378>
- The Use of Supervisory and Regulatory Technology by Authorities and Regulated Institutions. Market developments and financial stability implications. Financial Stability Board, Available at FSB: <https://www.fsb.org/wp-content/uploads/P091020.pdf>
- Vučinić, M., & Luburić, R. (2022). Fintech, Risk-Based Thinking and Cyber Risk. *Journal of Central Banking Theory and Practice*, 11(2), 27-53. Available at: <https://www.cbcg.me/repec/cbk/journal/vol11no2-2.pdf>
- Vučinić, M. (2020). Fintech and Financial Stability Potential Influence of FinTech on Financial Stability, Risks and Benefits. *Journal of Central Banking Theory and Practice*, 9(2) 43-66. Available at: <https://doi.org/10.2478/jcbtp-2020-0013>
- Zavolokina, L., Dolata, M., & Schwabe, G. (2016). The FinTech phenomenon: antecedents of financial innovation perceived by the popular press. *Financial Innovation*, 2(1), 1-16.
- Zeranski, S., & Sancak, I. E. (2020). Digitalisation of Financial Supervision with Supervisory Technology (SupTech). *Journal of International Banking Law & Regulation*. Available at SSRN: <https://ssrn.com/abstract=3632053> or <http://dx.doi.org/10.2139/ssrn.3632053>

