CSERNE PANKA PÓTA – PATRÍCIA BECSKY-NAGY

DISRUPTIVE SOLUTIONS FOR FINTECHS AND THEIR RISKS – HUNGARIAN CASE STUDIES

FINTECH CÉGEK DISZRUPTÍV MEGOLDÁSAI ÉS AZOK KOCKÁZATAI – MAGYARORSZÁGI ESETTANULMÁNYOK

In recent years disruptive technologies have transformed the traditional financial sector through their spillover effects into financial services. The aim of this research is to explore what disruptive solutions and business models are applied by the companies studied and what new potential risks they pose. The authors applied a qualitative research methodology to investigate four cases of Hungarian FinTech companies. They selected companies working in the most prominent FinTech areas in Hungary: an electronic payment service provider, an open banking and data aggregation company, an online payments risk analyst and a comparison platform company. This research findings confirm that the widespread disruptive technologies and business models mentioned in the literature are implemented in practice, which can also pose several novel risks. The most important risks are those related to the possible leakage of sensitive financial and customer data and the possible loss of control due to the use of AI.

Keywords: **FinTech, digital finance, cyber risk, cyber security, case study**

Az elmúlt években a diszruptív technológiák a pénzügyi szolgáltatásokra gyakorolt tovagyűrűző hatások révén átalakították a hagyományos pénzügyi ágazatot. A kutatás célja annak feltárása, hogy a vizsgált vállalatok milyen diszruptív megoldásokat és üzleti modelleket alkalmaznak, és ezek milyen új potenciális kockázatokat jelentenek. A szerzők kvalitatív kutatási módszertant alkalmaztak négy magyar FinTech vállalat esetét vizsgálva. A legjelentősebb magyarországi FinTech területeken működő vállalatokat választották ki: egy elektronikus fizetési szolgáltatót, egy nyílt banki és adataggregációs céget, egy online fizetési kockázatelemzőt és egy összehasonlító platformot üzemeltető céget. Kutatási eredményeik megerősítik, hogy a szakirodalomban említett, széles körben elterjedt diszruptív technológiák és üzleti modellek a vizsgált vállalatok gyakorlatában is megvalósulnak, amelyek számos újszerű kockázatot is hordozhatnak. A legfontosabb kockázatok az érzékeny pénzügyi és ügyféladatok esetleges kiszivárgásával, valamint a mesterséges intelligencia alkalmazásából adódó kontrollvesztéssel kapcsolatosak.

Kulcsszavak: **FinTech, digitális pénzügy, kiberkockázat, kiberbiztonság, esettanulmány**

Funding/Finanszírozás:
This paper is supported by the ÚNKP-22-23 New National Excellence Program of the Ministry for Culture and Innovation from the resource of the National Research, Development and Innovation Fund.

Jelen írás a Kulturális és Innovációs Minisztérium ÚNKP-22-23 Új Nemzeti Kiválósági Programja a Nemzeti Kutatási, Fejlesztési és Innovációs Alap forrásából valósult meg.

Authors/Szerzők:
Cserne Panka Póta[a] (pota.cserne.panka@econ.unideb.hu) PhD student; Dr. Patrícia Becsky-Nagy[a] (becsky.nagy.patricia@econ.unideb.hu) associate professor

[a]University of Debrecen (Debreceni Egyetem) Hungary (Magyarország)

The article was received: 02. 11. 2022, revised: 31. 03. 2023, and 03. 04. 2023, accepted: 06 04. 2023.
A cikk beérkezett: 2022. 11. 02-án, javítva: 2023. 03. 31-én és 2023. 04. 03-án, elfogadva: 2023. 04. 06-án.

In recent years, the use of digital applications, speed and electronic administration, and the demand for better customer experience have also become more common in financial services. Even before the pandemic outbreak, the sector was shaped by digital trends, with the demand for alternative payment models. Payment card use was the first alternative, but today there are many online payment options available for both traders and buyers. The pandemic has increased the digital presence of businesses and consumers, providing a new attack platform for hackers; thus, there is a growing need to protect customer data.

The actuality of the research topic is created by the fact that digitalisation has revolutionised the field of finance, and the impact of disruptive technologies in financial services has reshaped the traditional financial sector. Many innovations can be harnessed to deliver digital financial services. Due to the introduction of digital financial services (e.g., electronic payment), cyber risk factors have appeared in the data flow; thus, users' data must be handled with great care to prevent misuse.

We are witnessing a global revolution, as innovative solutions have become indispensable in many financial services worldwide (Droppa & Becsky-Nagy 2019). The pandemic has brought digital payments to layers of society that would not have been reached for years (Farkas et al., 2022).

Using case studies of four FinTech companies in Hungary, the research explores the disruptive technology used by the companies studied and assesses what we think the risks could be. The area of payment services is only one part of digital financial services, and our research will also focus on financial infrastructure providers and the risks arising from networking.

In our literature review, we briefly summarize the general changes in the digital financial sector, and also mention some disruptive technologies and business models used in FinTech. We describe the new potential risks posed by digital financial services and some security measures that can be used to counter financial cyber risks.

In our research, we have conducted four case studies dealing with four FinTech companies operating mainly in Hungary. Due to the small number of companies included in the case study, the research results are rather qualitative and cannot be used to draw generalised conclusions on the subject. The case studies will illustrate and evaluate the extent to which the disruptive technologies and business models mentioned in the literature are implemented in the practice of the selected companies. We have also highlighted the possible risks arising from the disruptive technologies and business models applied by the FinTechs studied when providing their financial services.

Literature review

A general overview of changes in the financial sector in the light of digitalisation

Digitalisation has changed consumer habits, with the need for a high level of customer experience coming to the fore, and most businesses have turned to technology to meet this need. Several new payment service providers have recently entered the market, offering a higher quality customer experience and exerting a massive influence on the relationship between incumbents (traditional financial players such as banks) and their customers – taking over some of the functions of traditional financial institutions (e.g. payment services) (EBA, 2018). Increased activity can be observed among the players challenging banks, not only in the B2C (business-to-customer) but also in the B2B (business-to-business) sector. B2B-focused financial service providers are increasingly seeking to support end-to-end transactions (KPMG, 2021).

The provision of financial services is heavily influenced by platformisation, including open banking efforts through the PSD2 (Revised Payment Services Directive) regulation and the expansion of so-called BigTech companies. Of the very large platform operators, the BigTech companies have the most significant market power and, in addition to their wide range of IT services, they have recently started to provide financial services.

PSD2, which was introduced in 2019, is an EU directive that paved the way for open banking. PSD2 obliges banks to provide access to their customers' accounts to external Third-Party Providers (TPPs), subject to their consent, to provide financial and information services. The primary objective of the directive was to strengthen competition in the banking market by involving digital financial service providers (e.g., FinTechs, BigTechs). The operating conditions for incumbents and digital financial service providers have been characterised by asymmetry from the outset. Traditional banks are subject to strict rules, while FinTech firms have mainly provided payment services using disruptive technologies at very low costs. Under PSD2's open banking rules, users decide with whom they want to share their financial data. Banks are responsible for ensuring that this sensitive financial data is transferred securely to financial service providers. The most appropriate tool for this is the open access Application Programming Interface (API) (Müller & Kerényi, 2021). Under the PSD2 rules, banks must make their API access available free of charge to the Account Information Service Provider (AISP) and Payment Initiation Service Provider (PISP) listed in the registers of financial authorities. These TPPs can connect to the bank's infrastructure via the bank's APIs. From here, they can retrieve transaction data and initiate transfers with the prior permission of customers (Németh, 2019a, 2019b).

Disruptive technologies and novel business models in the FinTech sector

Digital financial service providers use disruptive technologies (e.g., artificial intelligence (AI) and a subset of AI, machine learning (ML), or APIs to offer a higher-level customer experience. Understanding some of these innovations would require a high level of IT knowledge, so the IT side of these innovations is only touched upon in this article.

Using distributed ledger technology (DLT) for cross-border payments reduces process complexity and operational costs, speeds up reconciliation processes and enhances transaction transparency. It also increases the availability of KYC (Know Your Customer/Client) type data, making customer identification processes and thus risk management more efficient. However, if DLT-based payment systems fail to 'interoperate' with existing processes and infrastructures, this could lead to overall financial inefficiency (FSB, 2019).

BigTech companies have a massive number of users and, therefore, a vast amount of data, which they use to develop their platform strategy, taking over an increasing share of the financial intermediary system. They also have advantages in Big Data analytics tools (e.g., AI algorithms), which help them to better understand and influence customer needs (Müller & Kerényi, 2021). Increasingly sophisticated smart devices and their interconnection generate a staggeringly large amount of data. However, this data set has enormous value if processed with the right tools (e.g., AI).

Marketplace-type digital platforms where consumers can access a range of financial and non-financial products and services in one place are also becoming more common. The FinTech-enabled marketplace is based on a traditional marketplace business model with a FinTech solution (e.g., electronic payment, insurance, etc.) built directly into its platform. With this solution, a financial intermediary (e.g., an external payment service provider) – previously wedged between the buyer and the seller – can be removed from the process, strengthening the trust and business relationship between the trader and the customer (Flint, 2021). With the FinTech Marketplace, you can broaden your target market, and reduce customer acquisition costs, disruption, and friction during the ordering process, as the user manages everything on one interface throughout the entire purchase. An excellent example of a FinTech-enabled marketplace is Amazon (marketplace) which has a built-in electronic payment solution, Amazon Pay (Adevinta Ventures, 2021).

Risks posed by digital financial services

The use of FinTech can also present entirely new risks. The risk associated with AI-based solutions is that decision-making processes often occur without human intervention; customers and regulators do not fully understand how the algorithms work. Distributed ledger technology-based record keeping, and case management can blur legal and regulatory responsibilities based originally on bilateral agent-agent relationships. PSD2 removed one of the main functions of banks, the sole custody of banking secrecy based on the protection of customer data. Under the PSD2 open banking rules, TPPs can only access customers' account information after a strict identification procedure. However, it is difficult to check whether the TPP has also subcontracted services to another company, as this could result in sensitive customer data leaking from the given cycle. TPPs typically conclude such contracts for digital applications or new interfaces (Müller & Kerényi, 2021). However, customers' openness to artificial intelligence and promptness may reduce or mask risk sensitivity.

The financial sector has always been a popular target for cyber-attacks, but the pandemic has increased the digital presence of businesses and consumers, providing a new attack platform for hackers. Phishing and identity theft have become more common, and with the development of AI and ML, the technological sophistication of cyber-attacks has increased. Remote electronic banking has also become commonplace in banks, leading to the emergence of fraudulent activity related to the epidemic (MNB, 2021a).

In financial service processes, data can pass through many participants. Networking, or hyperconnectivity, is the phenomenon where all the participants involved in a given process are in a close, information-based connection. Thus, if one company's data in the network is compromised, this can have a negative domino effect on other companies' data. The interdependence of the participants in the network can be considered a weakness in contrast to the efficiency of information flow.

In markets where data is highly concentrated, the network effect is particularly large, and the costs of financial intermediation are reduced. Such market structures attract new entrants, but the resulting concentrated market power can be regarded as a disadvantage rather than an advantage. A prime example of this was when in November 2020, the US Department of Justice filed a lawsuit against the merger of Visa (a payment service provider) and Plaid (a FinTech data aggregator), which failed in early 2021. Each piece of data (e.g., payment information or a list of products viewed by a customer) has added value when combined with an existing huge data set. Therefore, data is more valuable to BigTech and similar firms with diverse businesses and high technology, which can develop into digital monopolies (Feyen et al., 2021). New infrastructures such as API platforms for payment and lending or distributed ledger technology systems can generate substantial network effects. They can transform or even eliminate the role of certain market participants (Arner et al., 2020).

Examples of security measures and methods to counter financial cyber risks

The use of new technologies has also increased the cyber risk to data. The EU introduced the GDPR (General Data Protection Regulation) to protect personal data. It was followed by PSD2, which includes several cybersecurity requirements, notably Strong Customer Authentication (SCA). This can help prevent phishing attempts because even if a customer's password is obtained, it is not enough to make a transfer because another authentication element (e.g., a fingerprint) is needed to initiate the transaction (MNB, 2020). From 1 January 2021, SCA is compulsory not only for electronically initiated transfers and physical bank card payments but also for online bank card payments. This means that when paying online, it is no longer sufficient to provide your payment card details and a confirmation code sent by SMS. However, the non-application of SCA is subject to an optional exemption rule for the initiation of remote electronic payment transactions, where the transaction monitoring mechanisms have identified the item as low risk. If the payment service provider makes use of the exemption rule, i.e., decides not to provide SCA, the customer's account manager is fully liable for any damage caused by the lack of such authentication. As the application of the exemption rules is left to the individual decision of the payment service providers, there may be differences in the practices of the account managers. As a result, customers have found that SCA is not always mandatory. SCA requires payment service providers to have transaction monitoring mechanisms in place to detect unauthorised or fraudulent payment transactions, but their real-time implementation is not mandatory. In view of the risks involved, the expectations of the Central Bank of Hungary regarding bank fraud prevention systems are different: banking systems must be able to detect payment attempts that are likely to originate from a source other than the legitimate owner of the funds or that do not follow the customer's usual transaction pattern in real-time, with a high degree of certainty (MNB, 2021b).

PSD2 required the European Banking Authority (EBA) to establish a central database – a register – of specific categories of financial firms (e.g., electronic money issuers, PSD2 service providers, etc.) providing services in EU countries. In cases where the financial service provider is not listed in the central register, the bank may block the API call made by the provider. It is of particular importance for banks, as it they who are primarily liable in cases of fraud, rather than TPPs (Németh, 2019a).

Online transactions can be carried out in two models. Many traders use the so-called three-party payment model because the first card acceptors socialised the market to this model.

In this model, a service provider for card acceptance is inserted between the trader (online store) and the customer in a given transaction. During the transaction, the customer is redirected to a particular payment interface, where they enter their payment card details and pay, upon which the trader receives a confirmation note. In this model, the card acceptor operating the payment interface is responsible for the security of the sensitive banking data provided there. In a two-party payment model, the customer remains on the trader's interface until the end of the purchase process, when the trader transmits the customer's payment card details to the acceptor in the background. In this model, the trader is responsible for data security. To be able to use the two-party payment model, the trader must have a system and certification that complies with the PCI DSS standard for card schemes. If the trader's system does not meet the requirements set by the standard, the trader can only make online payments in the three-party model (Schmidt, 2018).

The PCI DSS (Payment Card Industry Data Security Standard) is a set of requirements developed by the Payment Card Industry Security Standards Council. The standard was developed by Visa, MasterCard, Amex, JCB and Discover. It includes clear guidance for traders on the security solutions they need in order to manage card data. The rules ensure that online transactions are secure and that payment card details cannot be obtained by phishing.

Interpreting the well-detailed PCI documentation is a challenge for inexperienced professionals. Completing the 60-page self-assessment questionnaire and the level of certification required are not always trivial issues, so the involvement of external consultants and experts may be necessary for the implementation. Once successfully certified, the system will be subject to a regular review, which can only be carried out by a security company with the appropriate licence. The overall implementation process can amount to thousands of euros and the annual maintenance is also in the hundreds of euros, which is either unfeasible or financially burdensome for smaller retailers (Schmidt, 2018).

Methodology and data

Due to the novelty of the topic, the uncertainties and dynamic changes in the industry, and the limited amount of domestic and international data available, this research will be conducted using a qualitative approach to ensure effectiveness. To answer the research questions and to explore more profound relationships, our primary research involved preparing and reviewing a small number of subjects in the case studies. We have used four case study of FinTech companies in Hungary to illustrate the services, business models, data analytics tools and risk minimisation methods of the selected companies in the light of the trends, financial technologies, risks, and regulations presented in the literature. We have also highlighted the new potential risks arising from the disruptive technologies and business models applied by the FinTechs studied when providing their financial services.

One of the main criteria for selecting the companies was that they operate in different areas of activity in the FinTech market to showcase several possible application areas of disruptive solutions and explore risks in multiple areas. Focusing on the main areas of activity of the Hungarian digital financial sector, we selected Barion from the electronic payment service providers, FintechX from the open banking and data aggregation area, SEON from the online payments risk analysts and Bankmonitor from the comparison platform operators as the case study subjects. All four of the selected companies were included in the "25 most promising Hungarian FinTech companies" list published in 2016 (T-Systems, 2016) and in the "20 most promising Hungarian FinTech companies" list published in 2020 (FinTech Group, 2020).

We used various data collection tools to prepare the case studies, such as annual reports, internet sources and archives. In addition to the publicly available sources, we have included online in-depth interview materials with Barion's founder and CEO in the case study, enabling us to supplement our case study with up-to-date, primary source information.

The case studies are structured according to a pattern: the first section highlights the given company's main profile and outstanding successes, followed by a brief description of its products and services. Net revenue was converted at the 31 May 2022 exchange rate, the date which is the deadline for the disclosure of annual financial statements in Hungary. We will also address the security measures, methods, and regulations by which each business conducts its activities. Finally, for each company, we briefly summarise the disruptive technology that the company is using and what we think the new potential risk could be.

Due to the small number of companies included in the case study, the research results are qualitative and cannot be used to draw generalised conclusions on the subject.

Results and their evaluation

In recent years, FinTech companies have provided services in both B2C and B2B business models in Hungary. In the former category, the best-known providers in Hungary are Simple, Koin, Bankmonitor, Revolut, TransferWise and PayPal. The latter category is dominated by solutions that support the operations of traditional financial service providers, such as credit rating and fraud prevention. The best-known solutions are Blueopes, Aggreg8 (FintechX) and SEON. Most of these companies mentioned are increasingly strengthening their international presence in the digital financial market.

The Barion Payment case study

Barion Payment (*Table 1*) is engaged in electronic payment transactions in the retail and corporate banking, which was previously an activity exclusively associated with commercial banks. Barion is the first Hungarian company to have an e-money licence, which allows it to acquire retail and business customers faster with a simplified KYC process. In the corporate business, it provides card payment solutions for webshops (B2B) and P2P (peer-to-peer) money transfers (e.g., mobile payments) for the general public (T-Systems, 2016, FinTech Group, 2020).

Table 1

Barion Payment basic data

Barion Payment Zrt.			
Date of foundation:	30/06/2015	Net revenue:	1,006,512 thHUF 2,554.28 thEUR
Main profile:	Processing electronic payments		

Source: OPTEN (2022) authors' editing

Barion is one of the most promising FinTech companies in Hungary, with several FinTech activities. It was the first to introduce SCA in Hungary and to have an e-money licence. As part of its electronic money issuance activities, it operates its wallet, linked to a FinTech-enabled marketplace model. It allows traders using the service to sell products/services to their customers, who can then pay from their registered Barion wallet using Barion's smart payment gateway. According to Kiss (2021a), Barion is a combination of a FinTech and an AdTech (advertising technology) company. In the payment services sector, competitive advantage can be gained either through cost savings or through more efficient operations. Barion differentiates itself from incumbents on another front besides its cost-efficient payment service. When using Barion's smart payment gateway service, the merchant may choose to provide Barion with data on its customers for a lower fee, subject to their prior consent. Barion places great emphasis on monetising the data collected in this way, both to help the merchant to gain more customers and to generate a significant revenue stream for the business.

They differentiate themselves from other digital financial service providers in the domestic market with low transaction costs and fees, and data monetisation activities. In our view, the market position of FinTech companies is closely linked to the customer experience, which includes pricing. Therefore, providing services free of charge to the customer, which of course, brings revenues in the background, is a very effective way of attracting a large number of customers and thus gaining a larger market share.

Due to its PCI DSS certification, it can provide services in a two-party payment model while protecting customers' payment data. PCI is the highest level of expectation that Barion is required to meet. By incorporating the SEON tool (see more details in the SEON case study), a risk analysis is performed for all online transactions. If the result of the risk analysis shows that the payment is low risk, or the merchant wants to make the payment as smooth as possible for their customers, the merchant can request that no SCA is required for that payment. The card issuer may choose not to accept the merchant's request and still perform SCA, or it may choose to accept the merchant's request. If SEON's risk analysis shows that the transaction has parameters or facts that indicate that it may be fraudulent, Barion will reject the merchant's request to make the transaction a payment without SCA. If fraudsters are successful and the cardholder reports this, they can request a refund. There has been a major precedent in the course of Barion's existence, in which fraudsters have attempted to commit tens of millions of dollars' worth of fraudulent activity, most of which has been caught by the system. However, card fraud has fallen sharply since the introduction of SCA on 1 January 2021, and is now negligible compared to what it was before (Kiss, 2021a). In our view, Barion has introduced mandatory rules that provide a relatively high fraud prevention rate, but the company still cannot guarantee full protection against fraudsters.

They use their optionally implementable tool, Barion Pixel, to collect data for risk analysis and marketing activities, which they can use to understand their customers' habits better and thus provide a more personalised service. Through the way cookies work, an ML-based system can see what events users have been associated with or have carried out themselves. Based on these events and their parameters, the system classifies different users into different segments (Kiss, 2021a). It is, therefore, clear that Barion is taking advantage of the opportunities offered by Big Data. The various data processing and storage processes (e.g., payment card numbers stored in the system, customer data collected through cookies) also carry a fundamental risk of misuse. Barion has introduced mandatory rules that provide a relatively high fraud prevention rate, but the company cannot guarantee complete protection.

The FinTechX Technologies case study

FinTechX (*Table 2.*) was established in 2019 by the merger of the three companies shown below (Wyze, Aggreg8, FintechBlocks), whose founders have already presented their disruptive ideas in several FinTech fields. In late 2017, they received their first venture capital investment, and in 2018 their data aggregator solution won them the FinTech Show.

As the merged business entity retained the separate activities of the three participating companies, they are presented separately in the case study.

Table 2
FinTechX Technologies basic data

FinTechX Technologies Zrt.			
Date of foundation:	25/11/2019	Net revenue:	120,050 thHUF 304.66 thEUR
Main profile:	Open banking, financial data aggregation		
Wyze PFM Kft.	**Aggreg8 Kft.**	**FintechBlocks Kft.**	
13/12/2016	12/04/2017	21/04/2017	
Development of cost tracking and unbranded FinTech applications	Financial data aggregator, the first AISP in Hungary	API aggregator solution, banking innovation platform, supports PSD2 compliance	

Source: OPTEN (2022) authors' editing

FinTechX has been placed on the list of the most promising FinTech companies with three extraordinary ideas:

– Wyze's personal financial management app provides a user-friendly way to get an overview of your finances in relatively little time. The company is also involved in the development and unbranded resale of innovative FinTech solutions through other white-label development activities. According to the operator, data stored on Wyze.me is encrypted using state-of-the-art security measures. The data downloaded to the user's computer is sent to Wyze's servers via an https connection, and anonymised, including, for example, the username + transaction details (e.g. duckling2, Vodafone, 10 000 Ft). This anonymisation also provides protection if someone hacks into their server, as the hacker cannot know who the transactions of the duckling2 in the example belong to. This is possible because the company's CRM system, and thus the real or "masked" identities provided by the users, are physically located on separate servers, which do not interconnect in any way. Aggreg8 Ltd. is the operator and developer of the Wyze.me user interface, and therefore it – and the authority supervising it (Central Bank of Hungary) – guarantees the protection of data. Wyze's cost-tracking application handles sensitive financial customer data and protects against leaks using server-side synchronisation. As the founder admits, although it is much safer than the standard practice in Western countries, there is no guarantee that a phishing scammer cannot intrude into the download process.

– Among the merging parties, Aggreg8 was the first AISP registered in Hungary by the Central Bank of Hungary. Since then, in addition to Aggreg8, three companies have been awarded AISP licences (Turzó, 2019): Appspect/Recash, Számlázz.hu, and Zedna/Ginger App. FinTechX's Aggreg8 project is based on a financial data aggregator solution that provides contracted business partners with access to the banking data assets opened by PSD2. Aggreg8 can synchronise not only the transaction history of the customer's bank accounts but also the billing information of utility bills in one interface. Aggreg8, as a registered AISP, is entitled to access the account information of its bank customers – with their prior permission – and as a TPP, is an additional element of the information network, which can pose a risk according to the literature. In its RegComp service (license-as-a-service), Aggreg8 acts as a TPP between the business and its customer, to take the burden of legal compliance off the shoulders of the business, which would not have the right to access its customer's banking transaction data directly. Aggreg8 forms a three-party contractual structure between the business, its customer and Aggreg8, where:

- The business wants to use/integrate bank account information into its business processes and/or product/service offerings (e.g. accounting automation, credit scoring, tracking of invoice payments in the case of billing software, etc.) and therefore uses Aggreg8's RegComp service.
- Aggreg8, as a registered AISP, is entitled to access the invoice information of the client of the company, but in order to do so, the client must first contract with Aggreg8 to grant permission to access their data.
- The customer then grants Aggreg8 a mandate to share the bank account information received with the RegComp service provider in the context of an information sharing service.

So, as a TPP status company, Aggreg8 helps service providers to take advantage of the opportunities offered by the PSD2 regulation without using their own resources. In our view, it is a hazardous activity for Aggreg8 to transfer bank customer data within its RegComp service (with customer consent) to parties that do not have an authorised TPP status approved by the authorities. The security of the transfer of this banking data is determined on the one hand by the subjective judgement of Aggreg8 when contracting with an external partner, and on the other hand by the client's permission to transfer the data.

– The third participant in the merger is FintechBlocks, which creates a platform-as-a-service solution between banks and FinTech companies that can be easily connected to by either party, making the connection between FinTech companies and banks' systems faster and more efficient. By implementing the system, banks can also meet their legal obligations under PSD2. For data processing, FinTechX uses machine learning and other artificial intelligence-based solutions. FintechBlocks provides a cloud platform service, which would be considered risky in principle, but in the process, they build a private cloud inside the bank's firewall, connected to the bank's central systems, so it is not a public cloud but a kind of internal private banking network. However, bank employees' ethical and law-abiding conduct is the only way to prevent data from being transferred from an internal banking network to public or private networks.

The SEON Technologies case study

SEON (*Table 3*) offers fraud detection solutions for various industries: banking and insurance, online gaming and gambling, online lending, e-commerce, travel and ticketing, payment gateways, cryptocurrency, and commerce. For each industry, it provides a customised solution for a specific purpose. Of the industries just mentioned, only those related to finance were considered in our paper. On the financial side, SEON is developing a fraud prevention system that uses machine learning to filter out potential fraud in online transactions. Its clients include OTP Bank, Granit Bank and Barion, among others.

Table 3

SEON Technologies basic data

SEON Technologies Kft.			
Date of foundation:	10/01/2017	Net revenue:	673,826 thHUF 1710 thEUR
Main profile:	Risk analysis of online bank card payments and authentication points		

Source: OPTEN (2021) authors' editing

SEON has built a fraud prevention system offered to users in two fraud detection tools with different levels of analysis. During data collection, a risk profile is created, and the system expands into a complete risk profile based on existing data from various public and community sources. A given transaction is immediately classified during risk analysis using machine learning models. Their fully-fledged fraud management system analyses the online behaviour of the subjects and the digital fingerprint of the device used to log in. It enriches data in real-time, using, among other things, social media profiles. Only the more complex tool needs to be integrated (which takes a short period of time), and once activated, it immediately reduces the risk of transaction fraud. Through machine learning, the system continuously improves its efficiency by learning from previously detected fraud cases, and the user can customise almost everything (e.g., rights, risk assessment thresholds, etc.) through an API.

Barion and SEON have agreed to better combat cyber fraudsters who activate themselves during online card payments. SEON's fraud detection tool has been integrated into Barion's payment system, which can detect nearly 80% of card fraud attempts. Prior to the installation of the tool, Barion employees tried to filter out suspicious transactions during regular working hours manually, so suspicious transactions in the evenings and on weekends had to "wait". It quickly became apparent that a perpetual backlog is not sustainable in an online market where transactions occur 24/7. It was also essential for the growth of the business to keep the number of frauds as low as possible. Barion found the design of SEON's UX (user experience) and UI (user interface) extremely appealing, and the benefits of adding its fraud detection tool were immediately apparent. Due to machine learning, Barion's fraud detection system became increasingly efficient (Kiss, 2021b).

Even though SEON is a risk prevention company, its operations may still involve some risk. In our view, by integrating their tool in the transaction process, they embody another risk point, as sensitive information is passed through another participant.

During risk analysis, a transaction is immediately classified using ML models, but the decision process remains completely transparent. When scoring or levelling risk, there are predefined rules based on existing industry-specific data, but the user can also add new rules to the system, possibly company-specific ones. ML also creates new rules, which the user approves for inclusion. In the risk scoring process, the rules mentioned add or subtract a risk score for a given case, and then a final score is generated that can range from 0 to 100, where 0 is risk-free and 100 is the extreme risk level. When an online payment is made, if the system considers the likelihood of fraud to be high, based on the user's preferences, it automatically blocks the transaction. In the case of a lower risk of fraud, the merchant will receive an email about the suspicious purchase attempt, in which case it is recommended that the company uses, for example, the telephone as another channel to verify that the cardholder has indeed tried to pay with the card. To use SEON tools, one subscription is sufficient, access to the system can be shared between staff, and one can also personalise the privileges associated with the type of access. The risk assessment parameters of their fraud detection tool are – to a minimum degree – customisable and thus, in our opinion, can be manipulated to a small extent. The threshold at which a transaction is considered risky can be set higher, which we believe provides an opportunity for users of the tool to manually "pass" fraudsters through the check.

The Bankmonitor case study

According to FinTech Group (2020), Bankmonitor (*Table 4*) has wedged into the traditional distribution chain – between banks and their customers – following a classic marketplace logic, using a digital agent approach to help consumers quickly find financial products that best fit their individual needs. Its target market is the retail and SME market and financial service providers through its activities as an agent.

Bankmonitor helps users compare retail and corporate products with comparison platforms and their calculators and then helps the customer find the best, personalised offer and conclude a contract. With this end-to-end (E2E) solution, they assume a leading role among domestic non-bank service providers. The company is owned by Hungarian individuals who are entirely independent of banks, so their objectivity is guaranteed in this respect. The agency, multiple agency, insurance agency and membership agency activities related to certain products on the website are carried out by Bankmonitor Partner Ltd. under the supervision of the Central Bank of Hungary. For website visitors, the Bankmonitor service can be free of charge because the vast majority of its revenue comes from banks.

Table 4

The Bankmonitor case study

Bankmonitor Kft.			
Date of foundation:	14/12/2011	Net revenue:	342,642 thHUF 869.54 thEUR
Main profile:	Platform to help the comparison and selection of loan/deposit schemes		

Source: OPTEN (2022) authors' editing

From 1 January 2019, Hungarian law allows banks to identify their customers through indirect customer due diligence. So, you can open a bank account in non-real time, for example, by sending a selfie video or a picture, taking a photo of your identification documents and providing the relevant details electronically. In cooperation with Bankmonitor, the CIB Bank was the first financial institution in Hungary to offer its customers a discounted bank account opening service with an online process available all day long. The bank checks the application and, if approved, opens the account the next working day (FINTECHZONE, 2020).

Personal loan disbursements and bank account opening are now fully digital. The website also collects non-personal statistical data that cannot be used for individual identification through cookies for remarketing and website development purposes. In addition, the cookies also look at how users use the website, and what activities they have done there, in order to be able to send a more relevant offer to the customer. The system also saves the parameters of previously visited calculators so that the user can return to the page and continue the search where they left off.

Bankmonitor treats the information that comes to its knowledge in the course of its relationship with the client as banking secrecy in accordance with the relevant legal requirements and retains it without time limitation, even after the business relationship has ended. In its terms and conditions, Bankmonitor also describes that the purpose of the mediation agreement between the client and Bankmonitor – among other things – is to analyse and provide the client with competing financial services from at least three financial institutions, where such a volume is available on the market. In our opinion, the fact that Bankmonitor, as an external service provider, also handles data that constitute banking secrecy poses a huge risk, as the leakage of such data would provide fraudsters with opportunities for abuse and deception.

It is clear that Bankmonitor takes advantage of the benefits of Big Data to deliver the best possible customer experience for its users. In our opinion, a source of risk is that customers' non-personally identifiable data may still be identifiable to external third parties (e.g., Facebook, Google) in cases of transfers for marketing and remarketing purposes. In our view, a further risk factor would be implied if the objectivity guaranteed by Bankmonitor were to be compromised, as this platform, which is the dominant one in Hungary, could have a significant impact on customers' financial choices and thus on the competition between financial institutions in the market.

Conclusion

A summary of the case studies of the companies is presented in the table below (*Table 5*). All the examined FinTech companies work with disruptive financial technologies. The case studies clearly show that the disruptive technologies and business models mentioned in the literature are implemented in the practice of the companies studied. Based on the results, many of these FinTechs use machine learning and other AI-based solutions, and also take advantage of the benefits offered by Big Data to provide an even better customer experience.

From our standpoint, in addition to speed and efficiency, AI technologies applied to critical decision-making may raise the possibility of loss of control or deterioration in effectiveness. Phishing can also threaten financial service providers working with Big Data and their customers. In addition to violating customers' GDPR rights, the possible leakage of sensitive financial and customer data provides opportunity for abuse by fraudsters.

Infrastructure and cloud-based services, as well as the involvement of TPPs in processes, mean that sensitive information is passed through multiple participants. This kind of networking has a negative impact, as it provides hackers and phishers with more attack surfaces.

We have explored the changes in the financial sector due to digitalisation and the appearance of disruptive technologies and new business models which pose several novel risks. We have also collected examples of security measures and methods to counter financial cyber risks. After synthesizing the relevant Hungarian and international literature, we used the case studies of four FinTech companies in Hungary to illustrate and evaluate the extent to which the disruptive technologies and business models mentioned in the literature are implemented in the practices of the selected companies and what risks can arise when applying them. Based on the synthesis of the literature reviewed, it can be concluded that platformisation strongly determines the provision of financial services. Overall, it can be stated that several new potential risks are currently developing from the use of disruptive technological solutions and business models.

We consider that the cooperation of banks and FinTech companies is a crucial priority to preserve traditional values and facilitate the spread of disruptive technologies. An understanding of the fundamentals of disruptive financial technologies by employees and management would help to avoid inefficiencies in decision-making control resulting from the use of AI. The technological sophistication of cybercrime occasionally outstrips the effectiveness of protective measures, so the continuous improvement of cybersecurity measures is essential. Boosting the resilience of the financial system to cyber-attacks is a priority

Table 5

The summary of the case studies of the companies examined

Viewpoints	Barion Payment	FinTechX Technologies	SEON Technologies	Bankmonitor
Applied disruptive technology, business model	• e-wallet • the payment gateway for external and internal use • KYC • BigData • AI, machine learning • FinTech-enabled Marketplace • data monetisation	• PFM • AISP • API • cloud • white-label FinTech development • license-as-a-service • platform-as-a-service	• BigData • KYC • AI, machine learning • API • data enrichment • high-level UX, UI • online transaction fraud prevention	• BigData • comparative platform service • online calculator • digital agent and intermediary (E2E)
Sources of risk	• networking • leaks of sensitive financial and customer data • misuse of data, deception • loss of control due to AI	• an external party is involved in the process • networking • leaks of sensitive financial and customer data • misuse of data, deception • data transfer to participants that are not necessarily secure	• networking • leaks of sensitive financial and customer data • misuse of data, deception • manual fraud authorisation • loss of control due to AI	• manipulation by subjective advice • leaks of sensitive financial and customer data that constitute banking secrecy

Source: own compilation

to reduce systemic digital financial risks and protect consumers. Close cooperation between central financial regulators and cybersecurity professionals is also crucial to develop strategic and regulatory responses to cyber-attacks.

This paper studies the financial solutions and their risks in 2021, in four Hungarian companies only. Therefore, in a future work one should extend the scope of the study to the V4 countries or the European Union as well. An aspect of the future work could be the information-asymmetry on the financial market which distorts market mechanisms.

REFERENCES

Adevinta Ventures. (2021). *Fintech-enabled marketplaces – The future of marketplaces part two*. https://static.adevinta.com/wp-content/uploads/2021/09/22092204/Fintech-enabled-Marketplaces-2021-Adevinta-.pdf

Aggreg8. (2021). Data and information on the website. http://aggreg8.io/

Andor, M. (2017). *Fintech ragasztót fejleszt egy magyar startup* (Fintech glue developed by a Hungarian startup). https://FinTechzone.hu/FinTech-ragasztot-fejleszt-egy-magyar-startup/

Arner, D., Aurer, R., & Frost, J. (2020). Stablecoins: risks, potential and regulation. *BIS Working Papers No 905*. https://doi.org/10.2139/ssrn.3979495

Bankmonitor. (2021). Data and information on the website. https://bankmonitor.hu/

Barion Payment. (2021). Data and information on the website. https://www.barion.com/hu/

Droppa, D., & Becsky-Nagy, P. (2019). A pénzvilág üdvöskéi: a FinTech-megoldások. (The saviours of the financial world: FinTech solutions.) In *XIII. Pécsi Pénzügyi Napok – Új kihívások és lehetőségek. Konferenciakötet* (pp. 20-36). Pécsi Tudományegyetem Közgazdaságtudományi Kar, Pécs.

European Banking Authority. (2018). *EBA report on the impact of fintech on incumbent credit institutions' business models*. https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2270909/1f27bb57-387e-4978-82f6-ece725b51941/Report%20on%20the%20impact%20of%20Fintech%20on%20incumbent%20credit%20institutions%27%20business%20models.pdf?retry=1

Farkas, F., Póta, Cs. P., & Becsky-Nagy, P. (2022). Changes in payment patterns in Hungary during the pandemic. *WSEAS Transactions on Business and Economics*, 19, 1061-1074.
https://doi.org/10.37394/23207.2022.19.93

Feyen, E., Frost J., Gambocarta, L., Natarajan, H., & Saal, M. (2021). Fintech and the digital transformation of financial services: implications for market structure and public policy. *BIS Papers No 117*. https://www.bis.org/publ/bppdf/bispap117.pdf

Financial Stability Board. (2019). *Decentralised financial technologies – Report on financial stability, regulatory and governance implications*. https://www.fsb.org/wp-content/uploads/P060619.pdf

FinTech Group. (2020). *HUNFINTECH 20/20: A Magyar FinTech Book*. FinTech Group. https://FinTechzone.hu/wp-content/uploads/2020/05/HUNFINTEC_2020_MAGYAR_FINTECH_BOOK_e-book_WEB.pdf

FinTechX Technologies. (2021). Data and information on the website. https://FinTechx.digital/

FINTECHZONE. (2020). *Elindult a selfie-fotós számlanyitás a CIB Banknál. Otthonról, videóazonosítás nélkül nyithatunk bankszámlát* (CIB Bank has launched the selfie photo account opening. Open a bank account from home without video identification). https://fintechzone.hu/elindult-a-selfie-fotos-szamlanyitas-a-cib-banknal-otthonrol-videoazonositas-nelkul-nyithatunk-bankszamlat/

Flint, P. (2021). *The next frontier for 2-sided marketplaces: how fintech will unlock enormous value*. https://www.nfx.com/post/fintech-enabled-marketplaces/

Kiss, S. (2021a). *Online in-depth interview with the founding CEO of Barion Payment, Sándor Kiss.* Webex meeting, 2021. 10. 18.

Kiss, S. (2021b). *Barion – Leading payment gateway saves 50% work hours and keeps acquiring costs at bay.* https://seon.io/resources/case-study/barion-payment-gateway-saves-work-hours/

KPMG. (2021). *Pulse of Fintech H2'20*. https://assets.kpmg/content/dam/kpmg/xx/pdf/2021/02/pulse-of-fintech-h2-2020.pdf

MNB. (2020). *Fizetési Rendszer Jelentés* (Payment System Report). Magyar Nemzeti Bank, Budapest. https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2020.pdf

MNB. (2021a). *Fintech és digitalizációs jelentés* (Fintech and digitalisation report). Magyar Nemzeti Bank, Budapest. https://www.mnb.hu/kiadvanyok/jelentesek/fintech-es-digitalizacios-jelentes/fintech-es-digitalizacios-jelentes-2021-majus

MNB. (2021b). *Fizetési Rendszer Jelentés* (Payment System Report). Magyar Nemzeti Bank, Budapest. https://www.mnb.hu/letoltes/fizetesi-rendszer-jelentes-2021.pdf

Müller, J., & Kerényi, Á. (2021). Kiútkeresés a digitális pénzügyi innovációk labirintusában – A digitális pénzügyi rendszer szabályozási kihívásainak csapdája (Finding your way through the maze of digital financial innovations – The trap of regulatory challenges in the digital financial system). *Hitelintézeti Szemle, 20*(1), 103–126. https://doi.org/10.25201/hsz.20.1.103126

Németh, M. (2019a). Újabb fontos mérföldkő a nyílt *bankolásban: elindult az EU-s központi regiszter* (Another important milestone in open banking: the EU central register is launched). https://fintechzone.hu/ujabb-fontos-merfoldko-a-nyilt-bankolasban-elindult-az-eu-s-kozponti-regiszter/

Németh, M. (2019b). *12 nap a PSD2 indulásáig, de nincsenek megfelelő banki API hozzáférések* (12 days to PSD2 launch, but no proper banking API access). https://fintechzone.hu/12-nap-a-psd2-indulasaig-de-nincsenek-megfelelo-banki-api-hozzaferesek/

OPTEN. (2021) and *OPTEN*. (2022). https://www.opten.hu/

Schmidt, Z. (2018). *PCI DSS kereskedőknek: mikor kell tanúsítvány az online fizetéshez?* (PCI DSS for merchants: when do you need a certificate for online payments?). https://kosarertek.hu/uzemeltetes/pci-dss-kereskedoknek-mikor-kell-tanusitvany-az-online-fizeteshez/

SEON Technologies. (2021). Data and information on the website. https://seon.io/

T-SYSTEMS (2016). *HUNFINTECH25*. https://FinTechzone.hu/wp-content/uploads/2017/03/T_Systems_2016HunFinTech25_kiadvany.pdf

Turzó, Á. P. (2019). *Feltűnt négy magyar cég, amely felforgatná, amit a bankolásról eddig gondoltál* (Four Hungarian companies have emerged that could upend what you thought about banking) https://www.portfolio.hu/bank/20191220/feltunt-negy-magyar-ceg-amely-felforgatna-amit-a-bankolasrol-eddig-gondoltal-410197

Wzye.me. (2021). Data and information on the website. http://Wyze.me/index.html