ECONOMY AND FINANCE • VOL. 12. ISS. 3 • SEPT 2025 • DOI: 10.33908/EF.2025.3.2

REINFORCEMENT IN THE FIGHT AGAINST ONLINE CRIMINAL ACTIVITIES AFFECTING THE FINANCIAL SECTOR

Presentation of new legal institutions in cooperation between the public and private sectors

Gábor Jancsó[1]

ABSTRACT

Taking advantage of the digital financial habits that have changed in the wake of the coronavirus pandemic, the number of online frauds affecting the financial sector has begun to grow exponentially. This has resulted in the emergence of a qualitatively new criminal phenomenon that cannot be effectively addressed with the quantitative law enforcement solutions that were typically used in the past. However, the specific characteristics and capabilities of the financial sector make it possible to exploit new opportunities for cooperation between the public and private sectors (private-public-partnership, PPP system), which may be able to curb this phenomenon. This article aims to present the cooperation forums that have been established in relation to online fraud (KiberPajzs and the working group coordinated by the Ministry of Justice), as well as the functionality and added value of the PPP system. We also describe the results achieved, the measures introduced over the past year and a half, and the legal institutions: cooperation agreements between investigative authorities and banks, the Central Fraud Filter System, objective reporting, and information sharing.

JEL codes: G21, K14, K24, K42, O38

Keywords: online fraud, public-private cooperation, PPP system, financial service provider, crime prevention, law enforcement, cooperation agreement, KVR, objective reporting, information sharing

1 *Gábor Jancsó* is a correspondent author and former Deputy State Secretary for Criminal Legislation at the Ministry of Justice. Email:gabor.jancso@im.gov.hu.

1. INTRODUCTION – THE BASICS OF CRIMINAL JUSTICE

The author is a practicing criminal lawyer who believes that the state's monopoly on the use of force, the state's criminal law claims, the state's obligation to prosecute crimes, and the availability of the necessary tools are not a matter of debate or discussion, but rather an axiom that defines the foundations and framework of criminal justice. The rule of law and peaceful social coexistence are based on the principle that the state's claim in the field of criminal justice is essentially exclusive, and that the enforcement of individual claims is less tolerated. Justified self-defence and, in cases of extreme necessity, the enforcement of legitimate or perceived legitimate claims in an impermissible manner may even constitute a criminal offense.

Bibó writes in his treatise Ethics and Criminal Law: "The historical development of criminal law provides the strongest support for this interpretation of the function of punishment. The appropriation of private revenge by the community was the path through which criminal law developed. It was not the victims who first sought public protection against the criminals, but the defendants against the avenging relatives and the lynch mob. At the forefront of all criminal law dogma is the legal-historical observation that criminal law came into being whereby the public gradually took the right of retribution out of the hands of individuals. (Bibó, 1986, 174).

For criminal law, therefore, the state's system of tasks and guarantees is an indisputable fundamental principle, in light of which the regulatory logic of criminal law is that the state must provide the tools and resources necessary to perform the related tasks. Although our criminal procedure law[2] tolerates private investigation (specifically referred to as a defence right)[3] within the legal framework, it does not support it in substance, and there is no question of providing additional resources or sharing official resources and information. Even within the framework of the institutional system for correcting indictments, i.e., for correcting any deficiencies in the indictment (the victim acting as a supplementary private prosecutor, or, in the case of recently introduced priority crimes related to the exercise of public authority or the management of public property, a supplementary indictment that can essentially be filed by anyone in a separate proceeding)[4] , it is not guaranteed that a person who has been granted the right to bring charges alongside the state will be able to use the resources of the investigating authority. The state's

2 Act XC of 2017 on Criminal Procedure (hereinafter: Be.)

3 Be. Section 42(2)(c).

4 Be. Chapters CV and CV/A.

monopoly on prosecution therefore allows the victim or other authorized person to bring (supplementary) charges based on their different legal position or other information at their disposal, but the use and utilization of the investigative tools and the applicability of state coercion are no longer guaranteed. With the filing of charges, court proceedings and the adjudication of the matter by the court can therefore be "enforced," but the enforcement of the investigation and the use of the investigative authority's powers, tools, and resources for private purposes are not tolerated. Even in private prosecution proceedings, the use of the investigative authority's resources for extremely limited purposes is only conceivable for the purpose of establishing the identity of the person reported and exclusively under the supervision of the court.

It is therefore clear that the criminal justice system does not traditionally consider victims or other "civil" actors as partners.

In recent years, however, social trends have emerged that are fundamentally changing this operating mechanism. Advances in information technology and the challenges facing the financial sector have led to the development of new regulations and working methods in the field of law enforcement, with the criminal justice system beginning to view the private sector as a partner and the sharing of available resources becoming a requirement.

2 FORMS OF COOPERATION IN THE FIELD OF LAW ENFORCEMENT

Cooperation between law enforcement agencies and criminal sciences in the broader sense with other agencies and fields is not unprecedented. The use of criminal data and experience in urban architecture, for example, or cooperation with civil defence forces are not new forms of cooperation. Architectural crime prevention (Barabás ed., 2023) involves the criminological analysis of crime and the use of crime data – essentially data of public interest, crime statistics, and the scientific findings derived from them – so the "cooperation" and use of information is fairly one-sided. Cooperation with civil guards[5] and local civil initiatives is less strategic in nature and more a matter of supplementing the law enforcement capacities of the police (primarily in the areas of crime prevention and deterrence of offenders caught in the act); the institutionalized sharing of specific information from police criminal resources is not possible. At the same time, there is no

5 Act CLXV of 2011 on the Civil Guard and the Rules of Civil Guard Activities.

doubt that, in line with its objectives, this cooperation is capable of functioning at an excellent level and with great efficiency.

In our opinion, even these limited and very briefly presented cooperation solutions show that law enforcement agencies consider cooperation to be possible only at a general level, distancing themselves from individual criminal phenomena. In contrast, however, the forms of cooperation that have developed or are developing in the financial sector are qualitatively different, and we can speak of a real division of tasks and mutual sharing of resources/information.

3 CONDITIONS FOR THE DEVELOPMENT OF COOPERATION NEEDS IN THE FINANCIAL SECTOR

In order to bring about a qualitative change of approach in the financial sector in relation to public-private partnerships (PPP systems), the prevailing combination of several specific compelling circumstances and conditions was required.

3.1 Online fraud, a qualitatively new phenomenon in crime

First, it was necessary to recognize that online fraud represented a new social and criminal phenomenon. In previous years, when certain types of crime (mostly property crimes) were on the rise, it was found that certain phenomena could be dealt with relatively effectively by applying appropriate administrative and work organization solutions and by appropriately reallocating official capacities. For example, the proliferation of pickpocketing in the 2000s was successfully addressed by the establishment of a special police unit within the Budapest Police Headquarters, followed by an increase in the number of surveillance cameras; Car theft and the manipulation of car mileage were addressed by tightening the rules on origin checks, technical inspections, and registration[6]; the recent increase in grandparent scams[7] was addressed by awareness campaigns and increased police action, resulting in the arrest of the organizers.

A common feature of crimes that proliferated in space or time was that their spread was ultimately limited by physical constraints. Committing multiple crimes required more resources, mostly human resources, on the part of both the organizers and perpetrators. In addition, the resources used to commit the

6 https://www.mgoe.hu/nem-csak-magyar-betegseg-az-oratekeres-de-javul-tendencia.

7 https://vansegitseg.im.gov.hu/idosek-celkeresztben-igy-vadasznak-aldozataikra-az-unokazos-csalok.

crimes "only" proportionally increased the achievable "results." With the change in methods of committing crimes, the increase in crime primarily resulted in a quantitative change, which basically required a quantitative response (additional resources), and with appropriately innovative administrative solutions, it was even possible to achieve resource savings by making certain phenomena impossible (e.g., technical and administrative solutions that make it impossible to manipulate car odometers).

In contrast, in the case of online fraud, we are faced with a new type of crime, a qualitative change. On the one hand, in this case, the quantitative change in crime is essentially independent of the number of people involved in the commission of the crime. With IT solutions, an infinite number of attempts can be made to the detriment of an infinite number of victims, which does not require an infinite number of human resources, and the activity is not limited by space (Kovács–Terták, 2024). On the other hand, it can be said that it is difficult to imagine a system that cannot be circumvented, especially if the crime is committed by deceiving the victim, i.e., with the active participation of the victim (Biró–Kiss, 2024).

The "administrative" solutions that have proven useful in the past are thus less effective. Of course, it would be conceivable to tighten security measures (by shifting them to the offline space) to a degree that minimizes the risk of abuse, but this would undermine the essence and convenience of the current financial system and would not be compatible with the results of the digital revolution (Schenk, 2018). This path therefore does not seem viable; it is difficult to imagine a simple method that would make online fraud impossible from one day to the next while retaining all the innovative and convenient functions of online financial services.

Online fraud is therefore a qualitatively new phenomenon, and increasing the capacity of law enforcement agencies will not provide an adequate solution. A qualitative challenge cannot be addressed with a quantitative solution alone, so it is reasonable to look for an alternative solution, which is, in fact, more than obvious.

3.2 Lack of crime prevention capabilities and capacities in the case of cybercrime targeting IT systems

In addition to the urgent need to find alternative solutions, the evolution of the PPP system in the fight against online fraud has also been fundamentally determined by the specific characteristics and capabilities of the financial sector.

The author of this article first heard an interesting presentation on the potential of the PPP system and the related change in approach at a conference on cyber-

crime held in December 2020[8] . The essence of the presentation was that in the event of attacks on IT systems, the interests of the IT system operator and the law enforcement authorities are the same, IT knowledge is significant and indispensable on the part of the system operator, and thus the system operator can and wants to contribute substantially to the effective conduct of criminal proceedings. Although there are significant similarities between crimes that violate cybersecurity and online fraud that "exploits" the vulnerability of the financial sector, in the area of cybercrime that directly attacks IT systems, the public and private sectors are far from being able to develop the same level of strategic cooperation as in the case of online fraud affecting the financial sector.

In the case of operating IT security systems, two areas of interest can be identified on the victim's side, which fundamentally limit the possibilities for cooperation: either we are talking about an IT developer operating a system that has numerous customers (e.g., an operating system developer, a virus protection developer, etc.), or a given entity (business association, private individual) that operates its own IT system. In the first case, it is difficult to determine for what purpose the vulnerability of the system can be exploited, as users do not form a homogeneous system and can therefore become victims in many ways, for many reasons, purposes, and motives. The primary goal of the developer is to fix the current vulnerability of the IT system, regardless of the purpose for which it was used or could have been exploited, or the damage caused by the breach. In the case of entities operating their own/unique IT systems, it would also be difficult from a forensic point of view to generalize why the IT system of a given entity was attacked. The crime committed is fundamentally unique. In the cases presented, therefore, after the crime has been committed, there is indeed an interest in the effectiveness of criminal proceedings and a capacity for cooperation on the part of the developer and system operator, However, this is essentially a one-sided cooperation arising in a specific case, aimed at the success of the criminal proceedings, which does not differ in quality from the willingness and ability of the victims to cooperate with the law enforcement authorities. The peculiarity in this case is obviously the highly specialized professional IT knowledge identifiable on the part of the victims. However, there is no identifiable social or criminal phenomenon that could be effectively addressed through the cooperation of the actors. In terms of prevention and the prevention of future crimes – i.e., in a manner that is "backward" from criminal proceedings – meaningful cooperation is not really conceivable. The success of an attack on a given IT system ( ) is mostly independent of the vulnerability of other IT systems. The vulnerability that makes a given IT attack

8 V4CyberPower Conference 3-4 December 2020. https://iws.gov.pl/en/konferencja-v4cyberpower/

possible is mostly discovered by the developer or operator of the system itself, and law enforcement agencies cannot really add any significant value in this regard. Vulnerabilities identified and corrected in this way cannot be linked to future attacks that use completely new methods and exploit new vulnerabilities. In addition, the identified attack methods are IT solutions and data for which legal issues relating to data protection and the protection of private or other secrets are not relevant, so there is no obstacle to the developers concerned sharing their experiences with each other without any further involvement from the authorities. Once the vulnerability that triggered the security incident has been fixed, the specific method used to carry out the attack becomes impossible to use again. Finally, another fundamental difference is that in the case of attacks on IT systems, the group of victims (whether the developers of the IT system or the people using it) is so heterogeneous that it is not possible to identify a group of people for whom strategic cooperation aimed at addressing future vulnerabilities would be meaningful.

3.3 The financial sector's specific crime prevention capabilities and capacity

Unlike cybercrime targeting IT systems, online crime affecting the financial sector presents a unique situation:

- the group of people affected is clearly defined and homogeneous (businesses providing financial services),
- the aim of online fraud is not to attack the IT infrastructure of individual service providers (due to the different systems, we cannot speak of a homogeneous phenomenon), but to attack the users of IT solutions,
- unlike eliminating IT vulnerabilities, where closing a security gap eliminates the phenomenon, reducing the security risk of one user does not reduce the security risk of other users, and it cannot even be ruled out that a user who has been deceived before may become a victim of abuse again,
- the services provided to users by the financial sector and the solutions for using them are fundamentally uniform and can be developed uniformly (financial services),
- Perpetrators attack system users (customers) regardless of which financial service provider they belong to, whereby the entire financial sector is targeted by perpetrators through its large number of customers, and not just individual financial service providers.

– the solutions used in the commission of the crime are not unique (e.g., technical tools/solutions used to commit the crime, "money mule account numbers"[9], target accounts, cash withdrawal locations, etc. (Nagy, 2018)),
– the financial sector has significant resources and excellent professionals who operate and develop IT systems.

In this case, therefore, we are dealing with a mass phenomenon with homogeneous characteristics, in which

– specific characteristics of the offense,
– the capabilities and interests of the financial sector (Vass–Kovács, 2019),
– the capabilities and interests of law enforcement agencies

provided a real opportunity for strategic cooperation and division of tasks.

Strategic cooperation brings real added value to both parties involved (financial service providers and law enforcement agencies), because expert-level support for investigations is not only conceivable after a crime has been committed (as is also possible in the case of cooperation on information systems), but also in the prevention of future crimes. The latter means that, with the involvement of the state and the authorities, the financial sector's immune system can be significantly strengthened and enabled to prevent further abuses. Furthermore, the form of cooperation/task sharing on the part of the state/authorities can be not only general and methodological in nature (as in the field of architectural crime prevention, for example), but can also ensure the prevention of specific, individually identifiable fraudulent transactions. Through cooperation, financial sector players can play a meaningful role in the investigation and securing of assets derived from crime after the crime has been committed, while the authorities can play a meaningful role in preventing further abuses. The end result is mutually reinforcing, as not only can the effectiveness of criminal proceedings be increased, but the number of crimes can also be reduced, meaning that existing authorities' capacities can be utilized more efficiently and effectively. It would be vain to claim that online fraud can be eliminated in this way, but it can perhaps be said that it can be dealt with more effectively than with any previous unilateral solution.

9 Interim accounts that make it difficult to track funds, which are used periodically as collection accounts or for transfer purposes.

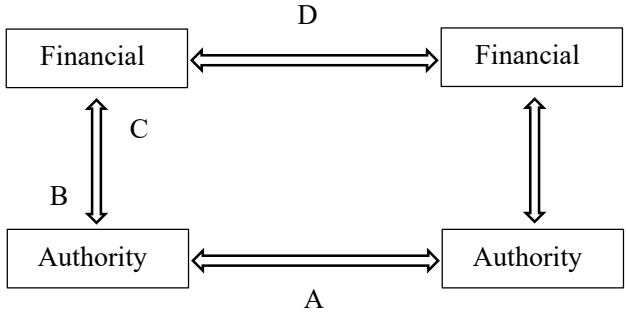
4 KEY POINTS OF THE PPP SYSTEM AFFECTING THE FINANCIAL SECTOR

There are two challenges to be addressed in the methodology of cooperation: information sharing (Vogel–Costa–Lassalle /eds., 2024/; EUCPN, 2023) and the efficient allocation of available resources.

4.1 Information sharing

There are four possible directions for the sharing of criminal intelligence affecting the financial sector *(Figure 1)*:

Figure 1
Directions of criminal information sharing affecting the financial sector



Source: own compilation

A: Information sharing between authorities is not new, and its framework is precisely defined by legal provisions. In the case of information sharing between authorities, there is no reason to differentiate according to the direction of sharing (which authority shares/can share information with which authority), as the regulatory logic is essentially the same: acting within the scope of its powers, the authority obtains and shares the information necessary for the performance of its tasks, when and under what conditions. In general, it can be said that the access of authorities conducting criminal proceedings is extremely limited (certain protected interests, such as operational interests or the classification of data for national security purposes, may constitute an obstacle to disclosure).

B: Information sharing between financial institutions and authorities can be divided into two parts according to the direction of sharing. The sharing of private information with authorities is also extremely limited. Apart from certain prior-

ity interests (such as attorney-client privilege), the authorities conducting criminal proceedings have access to essentially any data. It is typical for access to data to be subject to certain conditions (so-called external authorization), but this is not intended to prevent access, but rather to keep it within reasonable limits.

The basic logic behind the flow of information to the authorities is that data must be provided at the request of the authorities, and compliance with this request can be enforced. This logic follows from the tasks of the authorities involved in criminal proceedings and the coercive powers granted to them for this purpose. The novelty of information sharing in the PPP construct contains two differences in this respect. On the one hand, there is the sharing of information on one's own initiative (voluntary), and on the other hand, there is the increase in the effectiveness of information sharing in response to a request from the authorities (compulsory).

However, these cannot be considered qualitative innovations in terms of the possibility of information sharing, as the basic logic of the regulation has not changed.

C: The other direction of information sharing between financial institutions and the authorities, which points towards the private sector, does, however, represent a qualitative difference. The logic of official procedures does not typically involve the disclosure of information from their own systems. However, meaningful cooperation and the involvement of the financial sector in the prevention of crime is inconceivable without such information sharing. Of course, this cannot mean an unlimited flow of information; establishing a framework that is appropriate for the desired goal is a real regulatory challenge, and the framework for this had to be created.

D: Finally, the issue of sharing information and data managed in the private sector needs to be reviewed. In the financial sector, this issue is fundamentally limited by the strict and deliberately established regulations on data collection and banking secrecy, payment secrecy, securities secrecy, cash secrecy, and insurance secrecy (hereinafter collectively referred to as "financial secrecy"). The financial sector cannot become a huge database that can be managed without restrictions, in which financial institutions freely share and use each other's data to decide on the measures they deem necessary for prevention. The restrictions necessary for prevention (transaction bans) are part of the state's compulsory monopoly, and transferring them entirely to private hands, or "outsourcing" them, would raise fundamental issues of the rule of law. At the same time, effective PPP cooperation requires this type of information sharing, which also poses a significant regulatory challenge.

4.1 Efficient sharing of resources and tasks

Another challenge determining the viability of the PPP system is the effective division of tasks, the coordination of the tasks of the two sectors in line with their profiles, thereby ensuring the efficient use of the resources available in both sectors. It is necessary to develop an effective solution that is in line with the constitutional status of the actors involved and, at the same time, results in synergy in terms of its overall effect, i.e., it is not merely suitable for providing twice as many resources for a given task, whereby the task can be completed in half the time. This only means a proportional – quantitative – increase in resources, but, as we have already indicated, a quantitative response is not sufficient to meet the qualitative challenge of online crime.

While maintaining the constitutional framework, it is not acceptable, for example, to directly entrust the private sector with public tasks, official measures, and coercive measures. The state has a monopoly on the use of force, and public tasks related to law enforcement cannot be transferred. In addition to being one of the essential features of the state, the system of responsibility and guarantees associated with its application cannot be ensured, while the framework of official powers has become necessary based on centuries of experience. Like their clients, players in the financial sector belong to the private sphere, where equality is the norm and the system of responsibility is balanced. In contrast, official decisions and powers are characterized by asymmetry, and responsibility for the consequences of decisions is based on different legal grounds. In addition to the fact that vesting the financial sector with regulatory powers would have unforeseeable consequences, presumably including a loss of trust on the part of customers, a solution of this kind would not constitute an effective division of tasks, but would merely mean outsourcing the lack of regulatory resources to the private sector. Furthermore, it would be impossible to avoid developing the authorities, as outsourcing investigative tasks would lead to an increase in the number of criminal proceedings, meaning that the legal side (courts, public prosecutors) would also have to be developed. What is more, the criminal justice system would clearly be unable to cope with the burden of the expected increase in the number of criminal proceedings.

Such a solution would also inevitably lead to contradictions between the sectors, as the "short-term" interest of the financial sector would dictate that every single act be prevented or remedied, while the operational interest of the investigative authority would in many cases require the processes to be allowed to continue, at least temporarily.

The opposite extreme solution is also inconceivable: making the investigative authority's resources fully available to the financial sector in order to ensure the

secure execution of financial transactions, the prevention of fraudulent legal transactions, and the recovery of assets in the event of online fraud. Criminal proceedings are fundamentally retrospective in nature, and the state has a wide range of criminal law tools at its disposal because society has suffered (or is at immediate risk of suffering) harm that justifies the use of all these tools. The criminal law toolkit cannot be used for crime prevention purposes, or only to a very limited extent. In addition to the fact that the use of investigative tools to protect the interests of the financial sector – which are otherwise indisputable – would also violate fundamental constitutional principles, it would essentially divert the resources of the criminal justice system away from law enforcement. Thus, the criminal justice system would ultimately be unable to perform its task: investigating crimes and bringing perpetrators to justice (because perfect prevention is inconceivable). The use of investigative authority resources for this purpose is also insufficient from an efficiency perspective. The fragmentation of investigative resources—which focus on individual cases—would hinder the investigation of those who organize and direct crimes, develop methods of committing them, and provide the necessary technical means.

Instead of the deliberately extreme solutions presented, it would be more expedient to seek a solution that considers the natural organizational (self-)interests of the two sectors. It is difficult to argue that the financial sector's interest is to prevent individual abusive transactions (crime prevention), while the aim of criminal justice is rather to effectively detect crimes that have been committed and to hold the perpetrator(s) accountable (law enforcement). Accordingly, it is reasonable to divide tasks and resources in such a way that

1. significantly improves the crime prevention capabilities of the financial sector,
2. the prevention results (data) of the financial sector can also be applied in the field of law enforcement, and
3. the tasks performed or assumed by the financial sector reduce the pressure on the criminal justice system, enabling the authorities to better focus their available resources on their primary task of apprehending and prosecuting perpetrators.

This division of tasks, which is tailored to the specific characteristics of the sectors, is beneficial in several respects. On the one hand, it avoids mixing public and private law tasks and responsibilities. Accordingly, the tools necessary for crime prevention (or property insurance within the financial system) in the financial sector do not raise constitutional concerns, so the tools of the financial sector can be operated with significantly lower guarantee requirements. The division of tasks does not result in a confusion of roles on the part of financial sector employees, nor does it force decision-making that requires an official logic or approach.

Secondly, individual sectors can effectively deal with matters in which they have an interest, meaning that there is no need to develop separate motivational solutions or methods for measuring effectiveness. Effective crime prevention can result in a quantifiable reduction in losses on the part of the financial sector, which can serve as an objective measure of the effectiveness of the field. In the case of investigative authorities, no special motivation is needed to detect and successfully prosecute a major organized crime group, which can be greatly facilitated if their available resources do not have to be fragmented to track down individual fraudulent transactions.

5 COOPERATION FORUMS

There is therefore a qualitatively new phenomenon in which the actors involved (financial service providers, law enforcement authorities) have significant resources at their disposal, the novel coordination of which may indeed be able to provide a qualitative response to the challenges we face. In recent years, cooperation and the development of forms of cooperation have begun in several forums.

5.1 KiberPajzs – 2022

It is now widely accepted that the social changes brought about by the coronavirus pandemic and the increasing shift of our everyday lives to the online space have led to an exponential increase in online fraud, whereby.[10] The financial sector, which is directly affected, was the first to notice the change and scale of this phenomenon. It is therefore no coincidence that the need for joint action against this phenomenon also began as a professional initiative.

The KiberPajzs[11] cooperation platform was established in 2022 by the Magyar Nemzeti Bank (Hungarian National Bank), the Magyar Bankszövetség (Hungarian Banking Association), the Nemzeti Média- és Hírközlési Hatóság (National Media and Infocommunications Authority), the Nemzeti Kibervédelmi Intézet (National Cyber Security Institute) and the Országos Rendőr-főkapitányság (National Police Headquarters, hereinafter: ORFK).

Since then, several other participants have joined the initiative, including other government actors and the Ministry of Justice. Most recently, at the end of 2024,

10 https://www.mnb.hu/letoltes/1-fizetesi-rendszer-jelentes-2024-tovabb-fejlodik-a-hazai-penzforgalom-indul-a-qvik.pdf; Frész, 2025; Terták–Kovács, 2023.

11 kiberpajzs.hu.

the initiative expanded with the addition of Szerencsejáték Zrt., Mastercard, and Visa as professional partners.

This bottom-up professional initiative can function as a "soft tool" within the existing legal and organizational framework. Accordingly, cooperation between the public and private sectors has not been able to effectively address the challenges arising from the legal constraints of information sharing and task sharing described above. Nevertheless, the initiative was a milestone in the fight against online crime, as it made it clear to the actors involved that they had to work together whereby the phenomenon could be combatted. Within the existing legal framework, cooperation between investigative authorities and the financial sector could essentially aim at general knowledge sharing, exchange of experience, and the smooth operation of existing tools. The overall objective of KiberPajzs was to raise awareness, increase knowledge, protect victims, and share general knowledge related to the phenomenon. In addition, KiberPajzs's objectives also included the need to channel legislative proposals arising from professional cooperation to the government.

The work, results, and spirit of KiberPajzs greatly contributed to the signing of cooperation agreements between individual financial institutions and the National Police Headquarters.

5.2 Government working group coordinated by the Ministry of Justice – 2023

In addition to professional initiatives and cooperation, the social scale and impact of the phenomenon made it clear that the search for solutions could not be separated from a review of the existing legal framework and, if necessary, its reform, which would not be possible without government action. With this in mind, on the initiative of Minister of Justice Dr. Bence Tuzson, on December 14, 2023, a working group was set up with the support of the heads of the relevant government agencies, criminal justice agencies, and financial sector organizations. The majority of the bodies represented in the working group were also active participants in KiberPajzs, but the division of tasks between the two formations did not create unnecessary parallels.[12] Most of the bodies represented in the working

12 The consultation was attended by representatives of the Ministry of Justice, the Ministry of the Interior, the Ministry of Finance, the Ministry of Economic Development, the Hungarian National Bank, the Hungarian Banking Association, the National Court Office, the Prosecutor General's Office, the National Police Headquarters, and the Office for Combating Money Laundering and Terrorist Financing of the National Tax and Customs Administration.

group were also active participants in KiberPajzs, but the division of tasks between the two formations did not result in unnecessary duplication, but rather in an effective division of labor. The working group coordinated by the Ministry of Justice (hereinafter: MJ) was able to draw on the professional experience already gained by the financial sector within the framework of KiberPajzs, so that certain technical issues were already presented as mature positions in the government working group. On the other hand, the IM working group specifically aimed to develop appropriate legal frameworks and legal institutions that may have been lacking, so there was no overlap in the focus of the two working groups.

The novelty and effectiveness of cooperation between the public and private sectors was also evident in the activities of the working group. Despite the fact that preparatory work was underway on legislation specifically aimed at combating a criminal phenomenon, it proved extremely effective that the sectors concerned were able to participate in the search for solutions from the outset, whereby they helped to avoid futile, inherently unworkable or ineffective solutions. In addition, from the outset, the working group essentially carried out its work with a view to finding solutions and legal institutions based on the information sharing, effective cooperation and division of tasks described above, i.e. the separation of crime prevention and law enforcement between different sectors, which would have been inconceivable without the involvement of all stakeholders. Thus, in addition to increasing the effectiveness of criminal proceedings, the working group perhaps paid even greater attention to the issue of effectively managing the phenomenon outside of criminal proceedings, thereby reducing the burden on the criminal justice system.

Following the launch of the working group, several legislative amendments were made in the field of criminal law, specifically aimed at increasing the effectiveness of action against online crime (framework license, reform of jurisdiction rules, etc.). These amendments are part of the organic development of criminal law and have been developed in close cooperation with the professions involved in criminal proceedings, based on practical experience. Regulatory solutions that directly affect the effectiveness of law enforcement are important, and legislation must continue to be responsive to the professional needs that arise in this area. At the same time, in our opinion, the results achieved by the working group over the past year and a half represent real, qualitative progress. A number of laws have been enacted that affect both the financial and criminal sectors and can be seen as steps toward the cooperation between the public and private sectors and the sharing of information and tasks described above.

6 RECENT ACHIEVEMENTS RELATED TO THE PPP SYSTEM

6.1 Cooperation agreements

The beginning of strategic cooperation between the public and private sectors was marked by cooperation agreements between individual financial institutions and the National Police Headquarters. Cooperation agreements specifically aimed at effective action against online fraud were concluded with OTB Bank in November 2023[13] and with CIB Bank in early January 2025[14] .

The fundamental principle of cooperation agreements is that their content and the cooperation mechanisms they contain cannot exceed the existing legal framework, whereby. The cooperation agreement cannot therefore create rights, but it can ensure the effective functioning of existing legal instruments. The framework, legal basis and formal requirements for information sharing cannot therefore be modified, but it is possible to specify, for example, the channels and data request syllabuses that can greatly accelerate the flow of information. It is beneficial for all parties involved if the authority is familiar with the data sets managed by financial institutions, the mechanisms that make certain data sets more or less accessible, the parameters that enable data requests to be processed quickly, etc. Cooperation can be significantly accelerated if the authority knows what it can request, which data are immediately available, and how it can request the information in terms of labelling and format. Cooperation agreements may also aim at the reasonable planning of tasks, distinguishing between urgent and longer-term/tolerant cases, whereby helping to ensure that cooperation does not overburden the capacities of the financial sector.

Cooperation agreements cannot stretch the existing legal framework, so their conclusion does not actually require any special legal authorization. Cooperation agreements are "soft instruments," but their significance is extremely high. In addition to being able to significantly improve the practical application of existing legal institutions, whereby they provide tangible evidence that the parties to the agreement are equally committed to the task and treat each other as partners; this has led to a change in attitude on the part of the authorities in particular. With this in mind, the government wanted to support the spread of this initiative with clear legislative authority, based on the professional requirements that had already been raised in the working group coordinated by the Ministry of Justice.

13 https://www.portfolio.hu/bank/20231117/az-online-csalasok-ellen-kotott-egyuttmukodesi-megallapodast-az-orfk-es-az-otp-652277.

14 https://hvg.hu/gazdasag/20250108_banki-csalas-megallapodas-rendorseg-cib-bank.

Accordingly, Act LXIV of 2024 on the amendment of other laws necessary for further effective action against online fraud gave financial (and other) service providers (in connection with the investigating authority) the authority to conclude cooperation agreements in all legislation affecting the financial sector.

6.2 Central Fraud Detection System

The launch of the Central Fraud Filtering System[15] (hereinafter: KVR) is an extremely modern IT solution supporting the monitoring activities of the financial sector, but it is only marginally related to the issue of cooperation between the public and private sectors. Nevertheless, several features of the[16] system, which was launched on July 1, 2025, are worth mentioning in this context.

On the one hand, the KVR also seeks to share information relating to the financial sector. To this end, transactions passing through the GIRO Zrt. system are analysed and risk-rated. The KVR does not, therefore, involve the direct sharing or linking of the results of the monitoring activities of individual financial institutions. The monitoring activities of individual financial institutions, which also use artificial intelligence (Péter Bagó, 2023), essentially precede the KVR's assessment, as transactions considered risky by the financial institution in question are suspended and do not even reach the KVR for assessment. Of course, the data of transactions approved by the financial institution and then assigned a risk rating by the KVR are subsequently incorporated into the financial institution's monitoring system, so that ultimately the financial sector as a whole is able to utilize certain data and information. However, a financial institution's knowledge of a transaction that has been suspended cannot really be used directly in this system: on the one hand, because the KVR works with its own learning algorithm and not with the results of financial institutions, and on the other hand, because the suspension of the transaction by the financial institution does not even reach the KVR.

All this can be considered as maximizing the effectiveness of the applicable data protection and financial secrecy rules, as well as the scope of liability under private law. In addition, the KVR fits organically into the task-sharing logic of the

15 KVR is an artificial intelligence-based real-time transaction monitoring and evaluation system developed and operated by the Hungarian National Bank and Giro Zrt. The 2023 amendment to Act CCXXXV of 2013 on certain payment service providers ensures whereby the transfer of data by payment service providers to the KVR does not constitute a breach of payment secrecy.

16 https://www.mnb.hu/sajtoszoba/sajtokozlemenyek/2025-evi-sajtokozlemenyek/mesterseges-intelligenciat-vet-be-a-jegybank-a-penzugyi-kibercsalasok-visszaszoritasaert.

PPP system, as it can significantly improve the preventive capabilities of the financial sector, i.e., it can greatly reduce the burden on the criminal justice system with regard to individual transactions, allowing it to focus on perpetrators and organizers.

The KVR also raises exciting questions regarding the possibilities for further development within the PPP system. It will be interesting to examine the usefulness of the risk classifications identified by the KVR in criminal law, both in specific criminal proceedings and in criminal assessment and analysis activities. The operational logic of the KVR may be able to identify correlations between data arising in a specific criminal proceeding and additional transactions executed or planned to be executed in the financial system. In addition, the patterns and correlations identified by the KVR can also be used in law enforcement/criminal intelligence activities necessary for the initiation of criminal proceedings and in assessment and analysis activities carried out during preparatory proceedings (Nyeste–Szendrei, 2020; Nyeste, 2016).

Finally, it may be worth considering further developing the KVR in the PPP system from the perspective of how data arising from the authorities (whether in the fight against money laundering and terrorist financing or in the conduct of criminal proceedings) can be used in the KVR system.

6.3 Objective reporting obligation

Act XVIII of 2024 on the amendment of laws necessary to combat online fraud and other criminal laws amended Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: PTMT Act) with effect from 1 August 2024. amended Act LIII of 2017 on the prevention and combating of money laundering and terrorist financing (hereinafter: Pmt.) and introduced the legal institution of the so-called objective reporting obligation. Section 30 of the Pmt. stipulates that in the event of suspicion of money laundering, terrorist financing or other criminal offenses, those obliged to provide data (in this case, the financial sector) must report any data, facts or circumstances indicating such acts to the National Tax and Customs Administration's Office for Combating Money Laundering and Terrorist Financing (hereinafter: NAV PEI). Given that the report is based on the personal observations of the financial institution's employees, this form of reporting can reasonably be called subjective reporting.

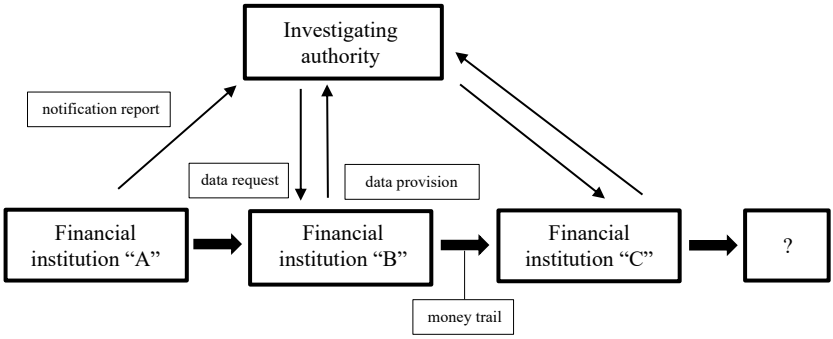
As of August 1, 2024, this form of reporting was supplemented by the new reporting form under Section 37/A of the Act. The law defines a payment transaction as a transaction affected by abuse – not including card-based payment transactions – in which there is reasonable cause to suspect fraud where the customer did not

intend to approve the payment transaction or where the customer approved it in error. In such circumstances, the law imposes a non-discretionary reporting and action obligation on the service provider, which is why this reporting form has become widespread in practice as an objective reporting obligation.

The legal institution was developed by a working group coordinated by the IM, based on the professional requirements that arose there. The monitoring activities carried out by financial institutions (or the recently launched KVR) are capable of preventing fraudulent transactions from being initiated. This is obviously the ideal situation, as in this case no harm is done, the transaction is not executed, the funds to be obtained remain in the detecting financial institution, and the crime remains unfinished. In such cases, the preventive action of the financial sector has been successful, and the criminal investigation department can begin investigating the crime and searching for the perpetrators, with no further harm expected in relation to the specific transaction. At the same time, it is clear that the prevention/monitoring system cannot identify and prevent all fraudulent transactions. In such cases, the financial institution is notified of the fraudulent transactions within a short or relatively short period of time. Practical experience has shown that money transfers between individual accounts, followed by the withdrawal of cash or transfer of funds abroad, can render the funds inaccessible within a very short period of time, a few hours or at most one or two days. It has been identified as a professional requirement that, if a fraudulent transaction is detected within a short period of time, either on the basis of a report by the victim or other information, a tool should be available to secure the funds still available in the financial system.

Given that we are talking about criminal offenses in these cases, it seemed obvious to expand the capabilities and capacities of the investigating authorities to a degree that would enable them to deal with the problem. Based on the classic logic of criminal proceedings involving cooperation with the authorities, the investigating authority communicates with those required to provide data in a "star-point" system. In other words, it identifies the next data subject (financial institution) on the basis of the incoming, acquired data, and then, after searching for it and processing the data received, it clarifies the next data subject (financial institution).

Figure 2
Schematic representation of the process



Source: own compilation

It is clear that in the world of online banking services, it is inconceivable to provide the level of resources or develop the level of cooperation that would be capable of competing with the speed of financial transactions in this data flow logic. The ability and willingness of financial institutions involved in the transaction chain to cooperate (report) is limited by the fact that they are typically unaware that the funds they have received or forwarded originate from fraudulent legal transactions. This information is only known to financial institution "A"; financial institution "B" only becomes aware of it when the investigating authority informs it of this in its request. Thus, apart from any independent alerts from the financial institutions' internal monitoring systems, other financial institutions involved in the transaction process are unable to take effective action, as they cannot identify the transaction as fraudulent without the relevant information.

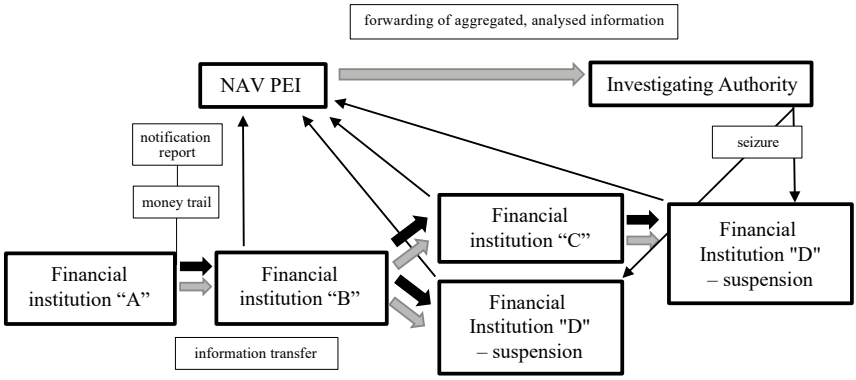
Another possible theoretical solution to this problem would be to grant financial institutions full authority to freely share data on financial transactions they deem fraudulent with other financial institutions, whereby ensuring that the funds remain within the financial system. However, in this form, it would not be compatible with data protection and financial secrecy rules, and it would also mean outsourcing the aforementioned state monopoly – and the responsibility that comes with it – which is to be avoided at all costs.

With all this in mind, a regulatory framework for objective reporting has been developed that is capable of providing an appropriate regulatory and accountability system, can be made operational with a reasonable expenditure of official resources, addresses concerns related to data protection and financial secrecy, and at the same time does not result in an unnecessary breach of the state monopoly on coercion or the outsourcing of state criminal law claims.

The cornerstones of an objective reporting system are:

- ensuring the possibility of sharing information between financial institutions involved in fraudulent transactions for specific purposes,
- automated IT solutions,
- NAV PEI, as the central authority in the system, ensures both the official decision and the integration and analysis of related data, while not burdening the investigating authority with the formality and other formal obligations of the procedure[17] ,
- the financial sector has the ability to temporarily withhold funds (suspend transactions),
- the securing of assets and their return to the victim already takes place within the framework of criminal proceedings.

Figure 3
Schematic representation of the objective reporting system



Source: own compilation

Essentially, the legal institution uses the legal framework, legal basis, and tools of the reporting obligation under the Pmt. and integrates them with the tools and institutional system of criminal proceedings. However, compared to subjective

17 Under the provisions of the Criminal Procedure Code, the authorities conducting criminal proceedings are obliged to initiate and conduct criminal proceedings if the legal conditions for doing so are met (officiality), but the initiation of criminal proceedings and the execution of individual procedural acts are only possible if the legal conditions are met. For example, based on the report, a decision must be made on whether to order an investigation, whether the conditions for coercive measures are met, or whether further data needs to be obtained, etc.

reporting, the Pmt. specifies the circumstances in which the financial institution is obliged to take action without further consideration (transactions affected by abuse). Another difference is that in this case, the financial institution not only reports to the NAV PEI, but is also entitled to inform the other financial institution(s) involved in the transaction. Moreover, in line with the speed of online banking services, the financial institution may first forward the information on the fraudulent transaction, and the reporting obligation only arises – retrospectively – on the part of the recipient financial institution.

The basic principle of the regulation is that the law prescribes an obligation to take action in the circumstances giving rise to the report. This obligation to take action also exists on the part of the NAV PEI, so that contacting/informing the financial institution involved in the fraudulent transaction would also be an obligation for it. The regulation "shortens" this legally required but unnecessary back-and-forth flow of information whereby direct information transfer is possible between the two financial institutions, while at the same time involving the authorities through the reporting process.

The compelling reason for directness and the reverse order of administration is clearly that otherwise it would not be possible to monitor online banking transactions and intervene in a meaningful way. The new tool is therefore necessary and proportionate to the objective pursued.

If other financial institutions are involved in the transaction chain, the obligation to transmit and report financial information shall be as described above. Therefore, if, as a result of the transaction, the funds received by financial institution "B" are transferred, financial institution "B" shall immediately forward the necessary information to financial institution "C" ( ), where the receipt of the information gives rise to a further reporting obligation. As a result of the information transfer process, which can be transferred and automated via IT channels, information on fraudulent transactions may be able to "catch up" with fraudulent financial transactions that are also carried out via IT channels and are also highly automatable.

As a result of the operation of this legal institution, if the funds are available at the financial institution at the end of the transaction chain, further disposal (further transactions) may be suspended and the assets secured, which is also a pre-existing legal institution regulated by Sections 34-35 of the Pmt. The suspension may be carried out by the financial institution, with a related notification, or on the basis of a provision by the NAV PEI. The suspension period is four working days, which may be extended by a maximum of three additional working days.

The NAV PEI summarizes and evaluates the transaction chain based on the reports of financial institutions. If no fraudulent transaction can be identified based

on the reports, the suspension will not take place or will be lifted immediately. NAV PEI forwards the information, supplemented where necessary as a result of its own evaluation and analysis (operational analysis pursuant to Section 39 of the Pmt.), to the authorities in aggregated form, having already processed it in substance pursuant to Sections 48-49 of the Pmt. NAV PEI performs risk-based activities and its operations are not bound by the constraints of measures affecting the authorities conducting criminal proceedings. Accordingly, NAV PEI has sufficient time to summarize and analyze the information received. If, on the basis of the information received, it can be established that the information on which the report is based is incorrect and the transaction is not fraudulent, it can take immediate action without unnecessary administrative burdens to ensure that the suspension is not imposed or that the suspended transactions are executed. In this case, there is no official obligation to forward the information to the authorities, thus avoiding unnecessary burden on the criminal justice system.

Finally, the NAV PEI's highly automated evaluation and analysis activities are not only capable of summarizing information on a given chain of fraudulent transactions, but also, where appropriate, of identifying links between several related chains of transactions. This is ensured by whereby the investigating authorities can treat cases that are related in terms of the perpetrators/methods of commission in a uniform manner from the outset and avoid having individual fraudulent transactions appear as separate cases in the system.

The actual securing – seizure – of assets is already carried out within the framework of criminal proceedings, by ordering coercive measures. The state coercive monopoly, which results in a substantive restriction of the right to private property, may also remain within the existing legal framework, with all known and functioning decision-making and responsibility competences, as well as guarantee and legal remedy elements. Based on the processing of the information forwarded by the NAV PEI, the investigating authority may examine the legal conditions for ordering an investigation and, in the event of a financial transaction being suspended, for securing assets (seizure, seizure). The information transmission process and the deadline for suspension specified in the Pmt. provide sufficient time for the investigating authority to assess whether it is justified to order an investigation and apply coercive measures.

In order to avoid the outsourcing of coercive measures, it is particularly important that, after the securing of assets, their return to the victims and the restoration of the original state remain the task and responsibility of the authorities. In practice, it is extremely rare for a linear transaction process to be halted by the transfer of information. It is more typical for funds to be divided, combined, or mixed with legal transactions between several financial institutions. In the case of a complex transaction chain involving a number of financial institutions, it is

obviously not reasonable to expect the financial institution suspending the transaction to investigate the origin of the assets and decide who can be considered the injured party and to what extent the existing funds should be distributed among them. However, the legal tools necessary for this are available within the framework of criminal proceedings, and the clarification of these issues fits into the "normal" schedule of criminal proceedings, so the authorities conducting criminal proceedings can be expected to perform such tasks.

An additional advantage of the objective reporting obligation is that the transmission of information can be automated on the part of the financial institution, the NAV PEI, and the investigating authority. The reported information is thus automatically processed and transmitted by the IT system so that issues requiring human intervention can be resolved as quickly and as well prepared as possible.[18]

The new legal institution fits in well with the operating logic and challenges of the PPP structure presented earlier. We have managed to ensure that reasonable and important legal restrictions on data management/information transfer within the financial sector do not hinder effective operation. The transfer of information remains purpose-bound and proportionate to the objectives set out in the law. There has been no outsourcing of the state's criminal law powers; the financial system's role is to temporarily secure assets related to fraudulent transactions, for no longer than the time necessary to make the necessary decisions in criminal proceedings. The transmission of information and the suspension of transactions are subject to official "control," with the NAV PEI providing the possibility of intervention if necessary. This is suitable for exercising appropriate control and supervision over possible abuses or erroneous measures, whereby, taking into account the subject matter and time limits of the interventions, it provides a sufficient and effective guarantee and corrective mechanism. In the case of coercive measures under criminal law that significantly restrict assets, a comprehensive system of legal remedies is already in place. Throughout the process, the rules of responsibility for individual civil and official actors are clear and in line with their organizational nature.

Finally, the new regulation also represents a significant step forward in the area of task sharing. Cooperation between financial institutions ensures the preservation of assets and the visibility of fraudulent transaction processes. In addition, the information shared between financial institutions in connection with a given fraudulent transaction can contribute to the further development and learning of

18 Reports are received and processed by the NAV PEI's automated IT system. The information forwarded by NAV PEI in an automated manner is received and processed by the ORFK Dante system (Digital Data Analysis and Investigation Support System). (https://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/helyi-hirek/dante).

the monitoring systems of individual financial institutions, thereby helping to filter out new fraudulent transactions and increase the effectiveness of the monitoring system. The legal institution is also capable of linking transaction chains that are related from a law enforcement perspective. However, this is no longer the task of financial institutions, but of the authorities, primarily the NAV PEI. At the end of the process, the criminal investigation authorities can begin to search for and prosecute the perpetrators by securing the assets and processing the structured information made available to them. The investigating authority is thus relieved of the burden of trying to track down individual fraudulent transactions using traditional criminal law tools on the basis of reports from victims; this task is performed by the financial authorities through the objective reporting system (and with significantly greater efficiency). The financial sector has thus become an active participant in law enforcement processes, while the reduced burden on the investigating authority allows for the prosecution of perpetrators and the effective investigation of the activities of the organizers.

The functioning of the new legal institution is obviously not perfect, and based on experience, there will always be room for improvement. Nevertheless, we believe that the effectiveness of the legal institution is demonstrated by the fact that, according to information from the National Police Headquarters, in the 11 months since its introduction, up to June 10, 2025, more than HUF 2 billion in bank account funds have been secured, which can thus be quickly returned to the victims, whereby.

6.4 Information sharing

The objective reporting system ensures the effective sharing of information and the possibility of intervention by the financial sector, the NAV PEI, and law enforcement agencies in relation to a given transaction process that has already been executed. Similar to the KVR, however, information and knowledge related to transactions that have been pre-screened by the financial institution and blocked in the internal monitoring system cannot be widely disseminated in this system. Data protection and financial secrecy rules do not allow individual financial institutions to share data they consider risky directly with each other, whereby they must use an intermediary. Although this solution may seem feasible, it would in fact result in the complete exclusion of certain customers from the financial system ("blacklisting"), which would raise regulatory, guarantee, liability, and fundamental rights issues that fall within the scope of public tasks.

Despite the legitimate objections raised by the rule of law, the need for information sharing has arisen for genuine professional reasons, as the most effective method

of prevention would be for a risk clearly identified by one financial institution to trigger an immune response from the entire financial sector almost immediately. One of the characteristics of online fraud is that it generates mass phenomena through IT solutions, i.e., it attempts to exploit the same method of commission on a massive scale whereby. If, after the first successfully identified fraudulent initiative or completed transaction, all further attempts using the same solution (technical device, "money mule account," target account, etc.) could be blocked, perpetrators could be deprived of the mass nature of online fraud. Such a high level of success in crime prevention could even reduce the "return" on the crime to such an extent that the resources required for further fraudulent transactions would no longer be proportionate to the expected profit. This could even lead to a natural decline and eventual disappearance of online fraud. The development of an effective and reliable immune response affecting the entire financial sector therefore promises significant results.

Act XLIX of 2025 on the amendment of laws relating to justice, adopted in the spring of 2025, aimed to meet this professional need. In this case, too, the regulation seeks to provide a solution to the problem by amending the Pmt. The regulatory system of the Pmt. already authorizes financial institutions to report suspicious transactions to the NAV PEI, whereby they are empowered to do so. However, if the financial institution is able to prevent the fraudulent transaction within its own system, based on its business regulations, it is not necessarily in the financial institution's interest to bear the administrative obligations associated with reporting. Reporting such information to the NAV PEI is no longer in the interest of the organization, but is motivated at most by the desire to avoid supervisory sanctions for failure to report. The lack of organizational interest stems from the fact that if the financial institution has already managed to block the specific transaction within its own jurisdiction, the reporting merely entails an additional administrative burden, while the further use of the report by the authorities is of no interest and uncertain. In contrast, whereby if financial institutions had specific knowledge that the information they transmitted would be directly useful to the entire financial sector, all financial institutions would have an interest in transmitting the information, since, on the one hand, they could rightly expect that the data shared by other financial institutions would next support their prevention and monitoring activities, and, on the other hand, they could rightly fear professional censure if it turned out that they had failed to transmit information that could be shared and thus help other institutions.

The new regulation makes it clear that the information on which the report is based can be returned by the NAV PEI to the financial sector almost immediately, after appropriate evaluation, whereby the financial institution's report will have a direct impact at the sector level. This element of the regulation is new. While the

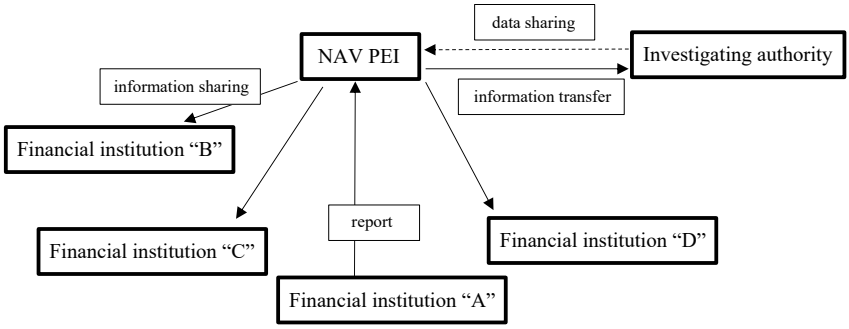
structured flow of information provided by financial service providers to NAV PEI has always been part of the institutional system, NAV PEI has not had the general option of "returning" information. Although it was possible to contact and intervene with specific financial institutions on the basis of the reports, it was not possible to share information in a general manner that would mobilize the entire sector.

In theory, general information sharing can be understood as a quantitative change in the current system. Based on its analysis of the information available to it, NAV PEI has the option of contacting certain service providers or suspending certain transactions based on information received from the service provider. Let us assume, whereby, based on this authorization, NAV PEI repeatedly sends requests within a very short time interval (every few seconds) to check data it considers suspicious, and then, if the service providers find a match, it automatically takes the necessary measures to suspend the identified transaction. Such an extremely resource-intensive theoretical solution can be considered equivalent to general information sharing in terms of its results. This solution would constitute an overload attack on financial service providers and the NAV PEI system, and at the same time would constitute an obvious circumvention of the original legal institution under the regulation. The quantitative modification would already be considered a qualitative difference, as there is a fundamental difference in terms of purpose, effect, and operation between a targeted search for specific information and a general, essentially continuous alert system, which would also require the constant availability of service providers. Accordingly, it is important to ensure that the new legal institution was not created by circumventing the existing regulations, but was given its own legal definition and regulatory framework.

The central element of the regulation is that NAV PEI has been granted legal authority to share information, whereby the usability of the shared information is limited in time. NAV PEI is a body performing a public function, with analytical capacity and the official powers necessary to achieve its objectives. The information shared in the financial service provider's report is subjected to appropriate checks (operational and strategic analysis) in the NAV PEI's own database, and thus the information can be shared with the financial sector as an official act, in accordance with the legal conditions. The responsibilities of the individual actors can be separated: the financial service provider reports its findings and the results of its monitoring activities to the NAV PEI. At this stage, it is responsible for the accuracy of the facts on which the report is based. The NAV PEI analyzes the content of the report, evaluates it against its own database, and shares it if the legal conditions (the purpose of the sharing) are met and the sharing of information is necessary to achieve these purposes. It is the official responsibility of the NAV PEI to assess the (substantive blocking) effect that the sharing of the information

on which the report is based will have on the transactions to which the information relates. After sharing the information, the NAV PEI has the additional task of deciding when and with what other information and analysis to forward the information to the investigating authorities.

Figure 4
Schematic model of information sharing (first round):



Source: own compilation

Financial service providers have access to the information shared by NAV PEI in a format that allows for automatic processing, enabling them to integrate it into their own monitoring systems in real time. Alerts related to information sharing may result in reporting obligations related to previous transactions or new transactions initiated after the information is received, or in the suspension of transactions. This means that the results of the monitoring activities of individual financial service providers can be used across the entire financial sector within a short period of time and can lead to the identification and sharing of new information related to fraudulent activities. The shared information can also be used in criminal proceedings and can help to identify the actions of perpetrators and track them down, while the financial sector is able to continuously prevent harmful consequences.

The logic of the information sharing system fits perfectly with the essence of the PPP concept. The resources of the financial sector are pooled and can be used effectively to prevent crime, while significantly reducing the burden on the criminal justice system. In addition, information on related attempts is available to law enforcement in an aggregated and processable structure, enabling the infrastructure behind the attempts to be dismantled and the perpetrators to be identified and held accountable.

Effective operation requires the system to be run by a suitably automated IT system, as the information flow model presented cannot be operated in a timely manner by human processing. The IT solutions developed during the operation of the objective system give reason to believe that the IT solutions necessary for the operation of this system will also be developed by the time the legal institution enters into force on June 1, 2026.

The logic of the system is that it works effectively if financial service providers carry out their monitoring activities efficiently, with adequate resources. We have already mentioned that service providers will be interested in information sharing not only because of their legal obligations, but also because they can expect to benefit from the data shared by other service providers, i.e., a voluntary agreement may develop regarding their interest in the joint operation of the system. At the same time, some service providers may gain an unjustified and abusive advantage if they neglect their own monitoring activities and seek to benefit solely from the information sharing of other service providers. This would minimize the costs of their monitoring activities, while allowing them to freely exploit the results of other service providers' resource investments with maximum efficiency. In addition to being a clear abuse of the mutual trust, responsibility, and reasonableness that form the basis of the system, it is also deeply reprehensible from a moral standpoint. It is clearly the responsibility of the government to create a regulatory and supervisory environment that ensures that all financial service providers are required to provide adequate resources and cooperation, and that they can only benefit from the results of the system's operation if they perform their assigned tasks properly.

7 SUMMARY

Based on the changes in online fraud over the past few years (social, IT, etc.), it can be said that we are facing a new phenomenon of crime and criminality. It is futile to assume that there is a solution that can completely eliminate this phenomenon. This could probably only happen if we eliminated the preconditions that enable the phenomenon to develop, which would mean giving up all the advantages, conveniences, and economically useful functions of current financial solutions. However, the extent of online fraud is still only measurable in thousandths of the total volume and value of financial transactions[19] , so such a

19 https://www.mnb.hu/letoltes/bartha-lajos-prezi-kiberpajzs-sajtotajekoztato-03-20.pdf; https://fintechzone.hu/a-kozponti-visszaelesszuro-rendszer-megvedheti-a-penzforgalmat-a-kibertamadasoktol/.

step backwards would clearly not be acceptable given the competitiveness of the economy and the popularity of the current solutions. The fight against online fraud as a whole is unlikely to be won, but that does not mean that battles cannot be won or results cannot be achieved. However, the new phenomenon of online fraud requires new methods and new forms of cooperation, and PPP cooperation, which is capable of making effective use of the financial sector's resources, should be given a prominent role in this.

The professional and governmental initiatives presented here have recognized in a timely manner that there is a need to coordinate resources and share tasks efficiently. We believe that the new forms of cooperation and legal institutions described above are steps in the right direction and promising initiatives that can serve as a basis for effective cooperation between the financial sector and law enforcement authorities, the further development of individual legal institutions, and solutions capable of responding to new challenges. However, it is essential to continuously monitor and evaluate the experiences of the processes that have been initiated. The forms of cooperation that have been established (Cyber Shield, government working group) can provide an appropriate forum for this work.

REFERENCES

Vogel, B. – Costa, E. – Lassalle, M. (eds., 2024): Law of Pubic-Private Cooperation against Financial Crime – Developing Information Sharing to Counter Money Laundering and Terrorism Financing; *Intersentia Ltd.* 2024. https://www.larcier-intersentia.com/en/law-public-private-cooperation-financial-crime-9781839704666.html.

Bagó, P. (2023): A kiberbiztonság és a mesterséges intelligencia kapcsolata. https://bankszovetseg.hu/Public/gep/2023/196-221%20Bago.pdf. (downloaded: 12.07.2025).

Bibó, I. (1986): Válogatott tanulmányok 1935-1944. *Magvető Könyvkiadó* 1986.

Biró, G. – Kiss, M. (2024): Adathalászat és az ellene történő egyes védekezési lehetőségek. https://bankszovetseg.hu/Public/gep/2024/G%C3%89P/417-440%20BiroKiss.pdf. (downloaded:12.07.2025).

Barabás, A. T. (ed. 2023): Kriminológia MA. Budapest: *Akadémiai Kiadó – Ludovika Egyetemi Kiadó*. https://mersz.hu/barabas-kriminologia-ma/. (downloaded: 12.07.2025).

EUCPN (2023): A köz- és magánszféra közötti partnerségek a bűnmegelőzésben: kihívások és ajánlások. https://eucpn.org/sites/default/files/document/files/Public%20private%20partnerships_Hungarian.pdf. (downloaded: 12.07.2025).

Frész, F. (2025): Az online csalások mögött álló bűnözői csoportok és kötődéseik. https://www.cyberthreat.report/p/az-online-csalasok-mogott-allo-bunozoi. (downloaded: 12.07.2025)

Kovács, L. – Terták, E. (2024): A kiberbűnözés legjobb ellenszere a pénzügyi műveltség. https://bankszovetseg.hu/Public/gep/006-029%20Kovacs_Tertak.pdf. (downloaded: 12.07.2025).

Nagy, R. (2018): A kibertérben elkövetett vagyon elleni bűncselekmények nyomozásának egyes kérdései. https://real.mtak.hu/120711/1/3850-Cikk%20sz%C3%B6vege-17536-1-10-20200721.pdf. (downloaded: 12.07.2025).

Nyeste, P. – Szendrei, F. (2020): A bűnügyi hírszerzés kézikönyve. (https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/A%20bu%CC%8Bnu%CC%88gyi%20hi%CC%81rszerze%CC%81s%20ke%CC%81ziko%CC%88nyve.pdf. (downloaded: 12.07.2025).

Nyeste, P. (2016): A bűnüldözési célú titkos információgyűjtés története, rendszerspecifikus sajátosságai, szektorális elvei. PhD. értekezés. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12375/Teljes%20sz%c3%b6veg%21.pdf?sequence=13&isAllowed=y. (downloaded: 12.07.2025).

Schenk, T. (2018): Digitális forradalom a bankszektorban. https://bankszovetseg.hu/Public/gep/2018/imp%20100-112ig%20Schenk%20Tamasuj.pdf. (downloaded: 12.07.2025).

Terták, E. – Kovács, L. (2023): Fókuszban a pénzügyi biztonság kibertérben is – Pénz7. https://bankszovetseg.hu/Public/gep/2023/005-020%20Tertak%20Kovacs.pdf. (downloaded: 12.07.2025).

Vass, P. – Kovács, L. (2019): A pénzügyi szektor szabályozásának aktuális kihívásai az európai unióban (2019–2024). https://www.bankszovetseg.hu/Public/gep/2019/413-430%20Kovacs%20Vass.pdf. (downloaded: 12.07.2025).