

UDK: 336.7 (439) 343.359 (439)
Professional paper

Tamás Károly Goricsán, PhD student
Faculty of Law, University of Pécs, Hungary
E-mail: goricsan.tamas@ajk.pte.hu
ORCID-ID: 0009-0004-1795-0771

THOUGHTS ON THE EFFECTIVENESS OF MEASURES AGAINST MONEY LAUNDERING

ABSTRACT

Hungary adopted, in Government Decision No. 1688/2017 (IX. 22.), an action plan for implementing the anti-money laundering recommendations made by the Moneyval. Based on Moneyval's fifth-round country report, Hungary was required to make appropriate progress in the areas of practical implementation and effective task performance. Furthermore, Act XLIII of 2020, amending the Criminal Procedure Act, redefined the money laundering as of 1 January 2021 in order to comply with Directive (EU) 2018/1673 of the European Parliament and of the Council. One of the typical forms of money laundering is committed by the so called financial agents. In many instances, the predicate offense is committed abroad, or the funds are transferred abroad from Hungarian transit accounts, thus necessitating cross-border criminal cooperation, evidence can generally be obtained only through judicial cooperation mechanisms. Eurojust serves as a forum for judicial cooperation, which investigating authorities can access through the public prosecutor's office. The International Law Enforcement Cooperation Center, operating within the National Police Headquarters, provides additional channels for police cooperation through Europol and Interpol. Data and information may also be obtained informally from foreign partner agencies, however, a formal request for legal assistance should not be omitted, even in such cases. Where a money laundering account is held at a foreign financial institution, an urgent request must be sent to National Tax and Customs Administration to contact the foreign partner and request the suspension of transaction. Accordingly, effective action against international money laundering is inconceivable without the exchange of cross-border information and data.

Keywords: money laundering, judicial cooperation, cross-border data exchange.

1. INTRODUCTION

Money laundering is a crime in which income obtained through criminal means is "cleaned" by returning it to the legal economy through secret, seemingly legal financial transactions. With the globalization of financial markets and the development of information technology, organized crime groups are increasingly able to hide illegal income and invest it in the financial sector.¹ Although money laundering does not have victims in the traditional sense, it has serious long-term consequences: laundered money sustains and finances organized crime and other serious crimes, while also fueling corruption and even terrorism financing in hidden ways. However, laundered illegal money does not only strengthen criminal circles.

Money derived from criminal activities undermines the integrity of financial systems and seriously jeopardizes public confidence. Money laundering distorts market competition, giving an advantage to economic actors who use illegal funds, while putting honest businesses at a disadvantage. This is harmful from an economic perspective, as the presence of fictitious capital can lead to a slowdown in economic growth and financial instability in the long term.

The fight against money laundering is a fundamental element of international law. The nature of money laundering is a crime relationship, and prosecuting perpetrators provides law enforcement with an effective tool in its fight against the predicate offenses, both in terms of detecting them and preventing the proceeds from being reused for criminal purposes.² Hungary is a signatory to the guidelines of the United Nations and the Financial Action Task Force³ (FATF) and is therefore obliged to implement the relevant conventions and recommendations. In addition, as a member state of the European Union, it is obliged to transpose EU anti-money

¹ Pintér, B., *A pénzmosás elleni küzdelem az új magyar büntető törvénykönyvben (Combating Money Laundering in the New Hungarian Criminal Law)*, doktori értekezés (doctoral thesis), Pécsi Tudományegyetem, Pécs 2012, p. 2.

² Belovics, E.; Molnár, G.; Sinku, P., *Büntetőjog II, Különös Rész (Criminal Law II, Special Part)*, ed.: Belovics, E., HVG-ORAC, Budapest 2021, p. 827.

³ The Financial Action Task Force is an intergovernmental organization that sets international standards for combating money laundering and terrorist financing. In order to protect the financial system from the risks of money laundering and terrorist financing and to ensure more effective compliance with international counter-terrorism strategies, the FATF identifies countries that have strategic deficiencies in their AML/CFT regimes. The organization calls on these countries to develop action plans and eliminate the identified deficiencies within a specified time frame. Financial Action Task Force, international standards on combating money laundering and terrorist financing, Hungarian National Bank website, <https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/korlatozo-intezkedesek-szankciok/penzugyi-akciocsoport-fatf>, 14 January 2026.

laundrying directives and regulations. In recent years, the EU has adopted a new regulatory package in the area of money laundrying and terrorist financing: In May 2024, the European Council approved new regulations that establish a European Anti-Money Laundrying and Counter-Terrorist Financing Authority and harmonize and tighten anti-money laundrying rules. The new regulations extend the scope of obligated financial and non-financial service providers, tighten the registration of beneficial owners and restrictions on the use of cash, and clarify the list of high-risk third countries.⁴ All this shows that the fight is becoming increasingly stringent within the EU framework and that cooperation between national institutions is deepening. In Hungary, the most important framework regulation is Act LIII of 2017 on the prevention and combating of money laundrying and terrorist financing.⁵ Hungarian legislation applies an international risk-based approach, which means that the risks of money laundrying and terrorist financing must be regularly assessed and identified. Since 2017, Hungary has been regularly preparing its national risk assessment, which outlines the greatest risks of money laundrying. Within the national institutional system, the Office for Combating Money Laundrying and Terrorist Financing (as the Financial Intelligence Unit, operating within the National Tax and Customs Administration, hereinafter: NTCA FIU) collects and analyzes reports of suspected money laundrying and forwards the data to competent law enforcement agencies.

The Hungarian National Bank and other specialized authorities supervise financial and investment service providers, while professional chambers monitor the customer due diligence obligations of non-financial professions (e.g., lawyers, auditors). The AML/CFT Act is therefore based on complex cooperation: financial sector players are required to analyze and report risks, supervisory authorities monitor compliance with regulations, and the judiciary enforces the rules through law enforcement activities.

In Hungary, the number of money laundrying crimes⁶ detected and registered in police proceedings has increased significantly in recent years. While the number

⁴ Information Note for Members of Parliament, Office of the Hungarian National Assembly, Public Collections and Public Education Directorate, Representative Information Service, No. 2025/18, 30 May 2025.

⁵ 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (on the prevention and combating of money laundrying and terrorist financing), Magyar Közlöny 2017/75., (hereinafter: AML/CFT Act).

⁶ This article does not aim to provide a detailed description of the current legal framework governing money laundrying. For more details: Gál, I. L., *Dogmatikai problémák a pénzmosás hatályos magyar szabályozásával kapcsolatban (Dogmatic problems related to the current Hungarian regulations on money laundrying)*, Belügyi Szemle, 71. évfolyam, 2023/5., pp. 741–763.

of money laundering offenses registered in the Unified Investigative Authority and Prosecutor's Office Criminal Statistics System was only 299 in 2020, this number reached 1,154 in 2024 and then 882 in the first seven months of 2025 (which predicted that the number of registered money laundering cases could exceed 1,500). However, the reasons for this increase are not only found in the proportional increase in the number of crimes (which is true, as the number of frauds committed online, which constitute the predicate offense of money laundering, and frauds committed using information systems has indeed increased⁷), but also to certain measures implemented to improve detection.

This professional article analyses this developments, with particular emphasis on the interaction between legislative reform and enforcement practice. The methodology of this study is descriptive and analytical; due to space constraints, I have not attempted to provide a critical, scholarly analysis of anti-money laundering measures. My primary focus here was on presenting the key legislative and other relevant measures that have made the fight against money laundering in Hungary faster, more effective, and thus more efficient for law enforcement agencies, while also providing an opportunity to learn about best practices and methods at the international level.

2. MAIN INSTITUTIONAL AND LEGISLATIVE MEASURES ENHANCING EFFECTIVENESS

2.1. Adopting the action plan against money laundering

Following the 5th round evaluation, the Hungarian Government adopted an action plan⁸ for implementing the recommendations made to Hungary by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (hereinafter: Moneyval). Based on the Moneyval 5th round country report, Hungary had to make appropriate progress primarily in the areas of practical implementation and effective task performance, to comply with this, the action plan defined tasks for the competent authorities⁹.

⁷ According to Unified Investigative Authority and Prosecutor's Office Crime Statistics, for example, the number of online fraud offences registered between 2021 and 2022 in police proceedings nearly doubled (from 6,344 to 11,389).

⁸ 1688/2017. (IX. 22.) Korm. határozat az Európa Tanács Moneyval országjelentésben Magyarország részére megfogalmazott pénzmosás elleni ajánlások végrehajtásáról készített akciótervről (Government Resolution on the action plan for implementing the recommendations against money laundering made to Hungary by the Moneyval), Magyar Közlöny 2017/153.

⁹ In addition, the Hungarian Government also adopted 1691/2018. (XII. 17.) Korm. határozat a pénzmosás és terrorizmus finanszírozása elleni nemzeti kockázátértékelés

The tasks assigned to the National Police Headquarters in the action plan included, among other things,¹⁰ the preparation of a methodological guide for investigative authorities, which would facilitate, on the one hand, the development of a uniform law enforcement practice for investigations initiated on suspicion of money laundering, and, on the other hand, to enable the separation of cases involving predicate offenses and money laundering, as well as the continuation of money laundering investigations even after the investigation of the predicate offense has been completed. In addition, it helps investigative authorities to focus on the highest risks, in line with the findings of the National Risk Assessment, and assists in the investigation of the most serious and sophisticated cases of organized money laundering.

This methodological guide¹¹ stipulates that the condition for establishing money laundering is a punishable predicate offense, which must be established at least at the level of simple suspicion.¹² Unlike the legal regulations of some other countries, Hungarian criminal law does not recognize the category of autonomous money laundering, i.e., when unusual transactions without any underlying crime can also be classified as money laundering.¹³

In this regard, data is needed to prove that the property originates from a punishable offense¹⁴ that is contrary to the specific provisions of the Hungarian

felülvizsgálata eredményeképp megfogalmazott intézkedésekről (Government Resolution on measures adopted following the review of the national risk assessment for money laundering and terrorist financing), Magyar Közlöny 2018/201.

¹⁰ The action plan against money laundering also called for increasing the capacity of the National Bureau of Investigation of the Riot Police, setting up an operational committee with the participation of law enforcement agencies involved in anti-money laundering, the organization of joint investigation teams, the review of legal practice, and the organization of multidisciplinary expert consultations and training.

¹¹ The author of this paper contributed significantly to the preparation of this methodological guide, as well as the methodological guide referred to later, which was initiated due to suspicions of social engineering fraud and the development of a uniform practice for investigating internet-based property crimes, and to support the specialized investigation of specific types of fraud.

¹² In Hungarian Supreme Court decision No. BH 2019.125, the court ruled that in the case of the predicate offense and money laundering, a genuine heterogeneous formal combination cannot be created, i.e., a single act cannot simultaneously fulfill the legal elements of the predicate offense and money laundering.

¹³ Gál, I. L., ed., *Magyar büntetőjog, Különös Rész (Hungarian Criminal Law, Special Part)*, Osiris, Budapest 2023, p. 511.

¹⁴ A criminal offense and a punishable offense are not synonymous. The commission of a criminal offense is an essential condition for the imposition of a penalty. Since the law uses the concept of a punishable offense (disposition-like offense), money laundering can be established even if the perpetrator's act is only disposition-like, but the perpetrator cannot

Criminal Code¹⁵; it can be e.g. a report by a financial service provider of an unusual transaction suspected of money laundering, a report by the victim, a report or message from a bank, a report by the NTCA FIU, a report by a foreign authority in connection with its own proceedings within the framework of international criminal cooperation, on the basis of which there is a simple suspicion of a criminal offense. The basic facts must therefore be proven to some extent in proceedings for money laundering. It is not sufficient to make assumptions or probabilistic inferences based on reports, it must be proven that the money actually derives from a punishable offense.¹⁶

In this context, it is necessary to emphasize that if, as a result of its evaluation and analysis activities, NTCA FIU provides the investigating authority with basic information on suspicious transactions and the use of straw men, on the basis of which a suspicion of money laundering can be established, an investigation (or, where justified, a supplementary report) must be ordered.¹⁷ Nowadays, an increasing proportion of crimes are committed using computers and the internet, and computers can also be a source of evidence. When defining crimes against property committed in cyberspace, it is necessary to consider which crimes fall within the narrower definition of crimes against property. In practice, two crimes from Chapter XXXVI of ACC fall into this category: fraud and fraud committed using an information system.¹⁸

According to Section 3(1)(d) of Credit Institutions Act¹⁹, the provision of payment services qualifies as a financial service. Pursuant to Section 6(1)(87), all activities necessary for payment and bank account management are considered payment services. According to Section 2(8) of Payment Services Act²⁰, an account opened

be punished for some reason, in Földvári, J.; Gál, I. L., *Magyar büntetőjog, Általános Rész (Hungarian Criminal Law, General Part)*, Osiris, Budapest 2024, p. 316.

¹⁵ 2012. évi C. törvény a Büntető Törvénykönyvről (Act on the Criminal Code), Magyar Közlöny 2012/92. sz., (hereinafter: ACC).

¹⁶ Gál, *op. cit.* note 13, p. 511.

¹⁷ A 2017. évi XC. törvény büntetőeljárásról (Act on the Criminal Procedure), Magyar Közlöny 2017/99. sz., (hereinafter: ACP) Part Nine provides for the possibility of initiating preparatory proceedings within the framework of criminal proceedings.

¹⁸ Separate criminalisation of damage caused using information systems in Hungarian criminal law, conceptual distinction from traditional fraud; however, it is necessary to regulate this conduct separately from fraud, as it does not involve misleading or deceiving others in the traditional sense. The damage is caused by the unlawful influence of the information system. Accordingly, the law regulates fraud committed using information systems as a separate offense in the chapter on crimes against property.

¹⁹ 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Act on Credit Institutions and Financial Enterprises), Magyar Közlöny 2013/217.

²⁰ 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról (Act on the provision of payment services), Magyar Közlöny 2009/100. sz.

in the name of one or more customers of a payment service provider for the purpose of executing payment transactions is considered a payment account, including a bank account.

In the case of money laundering [Section 399(2) and (3) of the ACC], the use of financial services constitutes a criminal offense only if it is related to property derived from the commission of a punishable act. Opening a bank account creates the possibility of subsequent financial transactions involving assets derived from the underlying act. Therefore, opening an account is generally not sufficient to establish criminal conduct, but a bank account opened in Hungary may, depending on the results of the investigation, prove the existence of an agreement concluded in Hungary for bank transactions involving sums derived from the commission of a punishable offense, and thus also the account holder's intention to cooperate in the predicate offense or in the related money laundering offense. The opening of an account in Hungary to be used for subsequent money laundering may therefore, even in the absence of conduct that can be assessed as criminal behavior, give rise to suspicion of preparation for money laundering in violation of Section 399(8) of the ACC and may constitute grounds for jurisdiction.

In addition to the above, depending on the outcome of the evidence, opening a bank account may also constitute aiding and abetting the predicate offense. The opening of a bank account or making it available may also be a prerequisite for the fraudulent, damaging basic act; without it, the victim's bank account could not be debited, so it must be examined whether the account holder was aware of the precise scope of the act; whether they understood the necessary connection between the damage caused as a result of the victim's deception and the making available of the bank account.

2.2. Relevant legal amendments

In the interests of effective action, Act XLIII of 2020 amending the CPA²¹ re-regulated the legal definition of money laundering as of January 1, 2021, in order to comply with 6AMLD.²² The new definition continues to punish all conduct that was punishable under the previous definition, but for clarity, it recodifies the individual basic cases in separate paragraphs without changing their systemic

²¹ 2020. évi XLIII. törvény a büntetőeljárásról szóló törvény és más kapcsolódó törvények módosításáról (amending the Criminal Procedure Act and other related acts), Magyar Közlöny 2020/129.

²² Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018.

significance. The amended provision aims to more effectively enforce the original criminal policy objective of criminalization, according to which crime can be more effectively curbed by preventing the financial gains from crime.²³ The most significant amendments are as follows:

- the range of money laundering offenses that can be committed by the perpetrator of the predicate offense has been expanded, as the material and intentional predicate offense of dynamic money laundering [Section 399 (1) and (2)] of the ACC no longer require the predicate offense to be committed by another person;²⁴
- more differentiated legal consequences are applied with the introduction of a system for classifying the value of the offense;
- instead of the object of the offense defined as a thing, the concept of property is used, which is not defined in either the ACC or the ACP;
- in dynamic basic cases [Section 399 (1) and (2) of the ACC], concealment is replaced by a new behavior, namely covering up, but this does not represent a substantive change;
- in the case of intentional dynamic money laundering [Section 399(2) of the ACC], the new conduct is receiving, using, concealing, disposing of, or participating in the alienation of property. In the case of self-laundering, these are distinguished from non-punishable subsequent acts by their intent. According to the detailed explanatory memorandum to the law, the common feature of these punishable acts is that, due to the fraudulent conduct associated with them, they go beyond the intended use of the property and cause additional damage;
- it highlights measures aimed at asset recovery and confiscation from the range of legal consequences for the perpetrator of the basic offense in cases of aiding and abetting [Section 399(3) of the ACC], while attempts to thwart other measures taken by the authorities in criminal proceedings are protected under criminal law through other legal provisions. This conclusion can only be reached if the criminal conduct is expressly aimed at avoiding the legal consequences related to the property;
- the basic case of aiding and abetting [Section 399(3) of the ACC] may also be committed by the perpetrator of the predicate offense, but only as a perpetrator [Section 399(9) of the ACC];
- the amendment repealed the offense of receiving stolen goods and integrated its criminal conduct into the basic case of static money laundering [Section 399(4) of the ACC]. In addition, the legislator

²³ Belovics; Molnár; Sinku, *op. cit.* note 2, p. 827.

²⁴ We speak of dynamic money laundering when the vast majority of criminal activities result in wealth transformation, whereas in the case of static money laundering, there is no such wealth transformation in economic terms, in Gál, *op. cit.* note 13, p. 512.

supplemented the acts constituting the basic case of static money laundering, adding a new element, namely the acquisition of the right of disposal, which is the contractual equivalent of the acquisition of property. The perpetrator of the predicate offense is not liable for this change either;

- all preparatory acts – not just the agreement to commit the offense jointly – are punishable [Section 399(8) of the ACC].

2.3. Other regulations relating to criminal proceedings

With regard to money laundering cases, the Department of Priority and Military Cases of the Hungarian Prosecutor General's Office issued Circular No. KF.9725/2004/379-II.²⁵ According to the circular, during the investigation, it is also a primary consideration that, in addition to measures taken to secure assets, all asset-generating (economic, or property) activities must be investigated to determine whether, after the completion of the predicate offense, the perpetrator of the predicate offense or another person committed any further acts in connection with the illegally acquired property that constitute money laundering in any form. If so, the investigation must be extended to include the crime of money laundering. One of the typical types of money laundering cases uncovered is money laundering committed by so-called financial agents. In these cases, the perpetrators typically agree with persons who remain unknown to open bank accounts or make their existing accounts available, with the understanding that they will transfer the money received in the account in exchange for an "agency fee" or withdraw it in cash and hand it over to an unknown person, or transfer it to a third country via money transfer services.

The perpetrator's state of mind can only be assessed based on all the evidence. Bank transactions carried out on behalf of and on the instructions of the principal in a bank account opened for someone else in the hope of receiving a commission conceal the identity of the person who actually controls the money, while the withdrawal of cash from the proceeds of the predicate offense serves to make it impossible to trace the assets, i.e., to conceal and hide the location of the money. It should be noted that, in the case of electronic transfers, typically made via online banking, the place of commission is the same as the place where the person initiating the transaction carried out the act. If this place is located abroad and the predicate offense is also suspected to have been committed abroad, then the

²⁵ Supplemented by Prosecutorial Circulars TPK.1008/2017/37-I and TPK.1008/2017/37-II.

territorial and personal jurisdiction of the Criminal Code must be examined in particular in relation to the investigation conducted on suspicion of money laundering (Hungarian jurisdiction must be examined separately in relation to the predicate offense and the related money laundering).

In most cases, it is not expedient to investigate crimes committed abroad by foreign nationals in Hungary, but if circumstances nevertheless justify conducting an investigation in Hungary, the initiation of criminal proceedings shall be ordered by the Prosecutor General pursuant to Section 3(3) of the ACC.

The Public Prosecutor's Office also took the position that the interrogation of so-called financial agents as witnesses is unlawful and, from a criminal tactics point of view, a flawed practice, since the conduct of such persons and their criminal liability should be examined as perpetrators of money laundering. During questioning as a witness, a person against whom there are well-founded suspicions of criminal activity may become aware of the ongoing investigation.

3. ENFORCEMENT PRACTICE AND THE ROLE OF FINANCIAL AGENTS

3.1. Practical experiences

Practice shows that in some cases the predicate offense is committed abroad by a foreign perpetrator, thus necessitating international criminal cooperation. Evidence that can be used in criminal proceedings can only be obtained through judicial cooperation. In addition to direct legal assistance channels, Eurojust is a forum for judicial co-operation, which can be accessed by the investigating authority through the public prosecutor's office. In addition to direct requests, it is also advisable to request data from financial service providers through the NTCA FIU, which also has links with countries outside the EU. In addition, the International Law Enforcement Cooperation Center (hereinafter: ILECC), which functions as an organizational element of the Hungarian National Police Headquarters, also provides channels for police cooperation (Europol and Interpol Hungarian Liaison Office), through which it is possible to exchange information directly with partner offices.²⁶

²⁶ For further details, see: 25/2017. (VIII. 17.) ORFK utasítás az Európai Rendőrségi Hivatal által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM–NGM együttes utasítás végrehajtásáról [Instruction of the National Police Headquarters on the implementation of Joint Instruction No. 23/2016 (IX. 15.) of BM–NGM on the

In addition to the above, it is also possible to obtain data and information informally from foreign judicial/law enforcement partner agencies, however, even in these cases, it is not possible to dispense with the initiation of a request for legal assistance (it is another matter that in the case of countries with which there is no reciprocity, or which, based on experience, would not comply with the request for legal assistance, or would do so only after a significant delay, no other data may be available apart from that obtained informally).

Experience shows that in the case of the method of committing the offense referred to as a financial agent or money courier ("money mule"), the basic act is usually committed in a foreign country, in many cases far away, outside Europe, using data obtained through an attack launched by means of a computer device. Identifying the perpetrator of the predicate offense is extremely time-consuming and costly, and would require law enforcement authorities to perform an impossible and, in the absence of jurisdiction, unnecessary task. As long as there is no evidence that a person who could be considered a defendant in a Hungarian criminal case – typically someone who has access to the account to which the money obtained through fraud is transferred – participated in the commission of the predicate offense, intentional conduct that could be considered money laundering should be assessed within the framework of Sections 399(1) and (2) of the ACC. The court of first instance did not assess the evidence in this regard.

3.2. The importance of seizure

Criminal proceedings must also cover the investigation of assets acquired through criminal activity and the application of coercive measures and sanctions of a financial nature.²⁷ The order of priority for seizure is as follows: first, assets credited to accounts, then cash, and only then movable property. Real estate may be used as security if the measures taken to recover damages are insufficient or unsuccessful.

If Hungarian jurisdiction does not extend to the criminal proceedings for the predicate offense, this does not in itself prevent the seized money from being

procedure for cooperation and information exchange using the applications of the European Secure Network operated by the European Police Office], Hivatalos Értesítő 2017/40.

²⁷ This is stipulated in Section 353 of the ACP, as well as in 20/2018 (V. 31.) ORFK utasítás a bűncselekményekből származó jövedelmek és a bűncselekményekhez kapcsolódó egyéb javak felkutatása, azonosítása és a vagyontbiztosítás érdekében teendő feladatokról (Instruction of the National Police Headquarters on the search for and identification of income derived from criminal offenses and other assets related to criminal offenses, and on tasks to be performed for the purpose of securing assets), Hivatalos Értesítő 2018/21.

released to the foreign victim, as the new crime committed against the object of the predicate offense against property (money laundering) does not affect the owner, and therefore does not affect the order of release following the termination of the seizure. In such cases, the object of the money laundering is the same as the object of the predicate offense, and there can be no confiscation of property, as this would make it impossible for the victim of the predicate offense to obtain compensation for the damage to their property rights.

3.3. Social engineering fraud

Nowadays, one of the typical methods of fraud is the so called social engineering fraud. Social engineering, or psychological manipulation, is when an authorized person transfers data to an unauthorized user or provides access to the system due to the deceptive behavior of the other person. Psychological manipulation is a type of attack in which the perpetrator does not exploit technological vulnerabilities, but rather uses human susceptibility as their main weapon. The most common form in international practice is Business Email Compromise (BEC/CEO fraud) as a prevalent form of international cyber-enabled fraud. Perpetrators typically hack into IT systems and trick employees responsible for financial transactions at the victim organization (business) into executing transfers according to false or forged payment instructions sent by them. Usually, they send a payment instruction on behalf of the partner from an email address created by the perpetrators that appears to be identical to the business partner's email address, requesting the fulfillment of a payment obligation relating to the actual business relationship to the company's changed payment account number, which is already under the control of the perpetrators. The crime can be committed not only with an email address similar to that of the financial partner, but also with their actual email address, by gaining unauthorized access to their account (compromising it). The methods used to commit these crimes are constantly changing, and nowadays there are also methods of fraud committed on a massive scale on social media and online marketplaces. Its significance, in connection with the commission of the basic act of money laundering, is outstanding.

4. INTERNATIONAL COOPERATION AND ASSET RECOVERY

In a significant proportion of cases, using the above mentioned social engineering fraud, as well as straw men, and in connection with drug trafficking or corruption, more serious, organized crime, the National Police Headquarters has prepared

another methodological guide under its professional supervision, which requires investigating authorities to carry out the following procedural actions:

- Pursuant to Section 368(1)(a) of the ACP,²⁸ the investigating authority is obliged, without a decision and regardless of its powers and jurisdiction, to carry out urgent investigative actions that cannot be postponed and may carry out any evidentiary acts that it would otherwise be authorized to order, and then send the resulting documents to the investigative authority with jurisdiction and competence.

In this context, if the target account is held by a financial institution operating in Hungary, immediate action must be taken to seize the incriminated amount for the purposes of indemnification. If it has already been withdrawn in cash, an immediate attempt must be made to seize it from the person concerned. In addition, if it is necessary to contact the domestic financial institution to obtain documents relating to the account or online banking data used, a request for information must be sent to it. The account-holding financial institution can be identified based on the first eight digits of the account number, for which several online platforms are available (e.g. bankkereso.eu). It is advisable to carry out the data request as an urgent investigative action [Section 262(3) of the ACP], as obtaining the prosecutor's permission would cause an unreasonable delay that would jeopardize the identification of the perpetrator or the collection of evidence. The following may be carried out within the framework of the data request: obtaining data related to the account number, identifying the characteristics of the accounting, payment and/or settlement system, suspending the operation, identifying suspicious financial partners, collecting data related to the beneficiary and listing the locations of cash withdrawals.

In case if the target account is held at a financial institution operating abroad, the investigating authority shall, also for the purpose of securing assets, send an urgent request to the NTCA FIU²⁹ in order to send a request to the foreign partner authority and to request the suspension of the transaction³⁰ from the foreign partner authority. The NTCA FIU shall

²⁸ Also based on Section 6(1) of 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről (Minister of Interior Decree on the powers and jurisdiction of police investigative authorities), Magyar Közlöny 2013/104.

²⁹ Pursuant to Section 48(4) of AML/CFT Act, authorities to which the NTCA FIU may independently forward information are entitled to send requests for the provision of information.

³⁰ The NTCA FIU can provide information on whether the national legislation of the requested country allows for the suspension of transactions, and on the time period during which it can maintain property insurance.

request the suspension of the transaction if, based on the facts of the case, the investigating authority's request establishes a suspicion of money laundering or an organized property-generating crime and the transfer to the foreign target account took place within three days.

If the investigating authority also requested the suspension of the transaction by the foreign partner authority in its request, this must be followed by the issuance of a European Investigation Order (hereinafter: EIO) or a request used in the Act on criminal cooperation with Member States of the European Union.³¹ It is important to note that neither reciprocity nor double criminality is a general condition for criminal cooperation with EU Member States. The Act however, applies the principle of double discrimination to some extent to certain forms of cooperation with other EU Member States.³²

According to the Act on International Legal Assistance in Criminal Matters³³ international treaties have priority compared to the application of the domestic regulation. Hungary has plentiful bi- and multilateral convention related to cooperation in criminal matters with other countries.³⁴ The confiscation of assets and freezing³⁵ for the purpose of compensating the victim for damage and/or financial loss does not fall within the scope of the EIO Directive and is only possible by means of a request for legal assistance or a decision ordering the freezing of assets.³⁶

- In order to obtain or change cross-border data and information, it is also necessary to involve ILECC, which may justify sending a request or submitting a request for legal assistance to the law enforcement authorities of the country concerned through European Police Office (hereinafter: Europol) and International Criminal Police Organization (hereinafter: Interpol) channels. Data obtained through informal channels can simplify and speed up requests for legal assistance, as data obtained through the SIENA system operated by the Europol, which ensures

³¹ 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről (Act on criminal cooperation with Member States of the European Union), Magyar Közlöny 2012/160.

³² Ligeti, K., *A Nemzetközi Bűnügyi Együttműködés Általános Feltételei (General Conditions for International Criminal Cooperation)*, in *Az Európai Bűntetőjog Kézikönyve (Handbook of European Criminal Law)*, ed.: Kondorosi, F.; Ligeti, K., Magyar Közlöny Lap- és Könyvkiadó, Budapest 2008, pp. 59-85, 76.

³³ 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről szóló (Act on international legal assistance in criminal matters), Magyar Közlöny 1996/54. sz.

³⁴ Köhalmi, L., *A Nemzetközi Bűnügyi Együttműködés (International Criminal Cooperation)*, in *Magyar Bűntetőjog Általános Rész (Hungarian Criminal Law General Part)*, ed.: Tóth, M.; Balogh, Á., Osiris, Budapest 2010, pp. 375-386, 376.

³⁵ This legal institution has been in force since December 19.

³⁶ Practical advantages of involving the NTCA FIU in urgent asset-freezing cases.

secure information exchange, can be obtained through a request for legal assistance and thus used in open proceedings.

Within ILECC, the Europol Hungarian Liaison Office carries out and supervises the exchange of information and the sending of requests within the framework of the above-mentioned Instruction No. 25/2017 (VIII.17.) of the National Police Headquarters. Based on this, several units were granted full access, and end-point users are able to engage in cross-border cooperation with partner agencies directly, without the involvement of the liaison office.

Europol has a separate unit dedicated to cybercrime (European Cybercrime Centre-EC3). Its work is carried out through three main analytical projects such as AP Cyborg, AP Twins and AP Terminal. Representing Hungary, the National Bureau of Investigation of the Riot Police³⁷ is a member of all three projects.

Interpol, which currently has 192 member countries, can mainly assist in the fight against cybercrime through international criminal cooperation with third countries. Information can be exchanged with Interpol via the "Interpol channel", typically with non-EU countries. The Hungarian National Office of Interpol, operating within the organizational framework of ILECC is authorized to maintain contact.

Liaison offices³⁸ also enable the direct exchange of data and information, among which the cybercrime liaison points are particularly noteworthy, through which the countries participating in the network operate a continuous, so-called non-stop on-call system for receiving and sending requests. Basically, ILECC is the designated 24/7 contact point, while the National Bureau of Investigation of the Riot Police acts as the professional contact point.

Cross-border data exchange through the network of liaison officers³⁹ – Europol Hungarian Liaison Office (Netherlands), Germany, Serbia,

³⁷ The Riot Police operates under the direct control of the National Police Headquarters – specifically, the Chief of the National Police – with independent tasks and powers, national jurisdiction, and as an independent central budgetary agency, in accordance with the tasks and powers specified in Section 9 of 329/2007. (XII. 13.) Korm. rendelet a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről (Government Decree on the Police and the tasks and powers of the Police), Magyar Közlöny 2007/174.

³⁸ Details regarding the rapid international exchange of information provided by the Liaison Offices (competent offices, mandatory elements of requests, areas of cooperation and information exchange) are available on the internal intranet website of the National Police Headquarters. For more details, see 11/2024. (III. 21.) ORFK utasítás a kapcsolattartási szolgálati helyek működéséről (Instruction of the National Police Headquarters on the operation of liaison offices), Hivatalos Értesítő 2024/16.

³⁹ For more details, visit <https://www.police.hu/hu/a-rendorsegrol/testulet/teruleti-szervek/nemzetkozi-bunugyi-egyuttmukodesi-kozpont>, 8 January, 2026.

United Kingdom and Southeast European Law Enforcement Center (SELEC) – can also support the success of the proceedings.⁴⁰

- In cases where reports are filed on the basis of a simple suspicion of a criminal offense, an investigation must be ordered within the time limit prescribed by law; there can be no supplementation or rejection of the report. In cases of online fraud, to identify the perpetrator(s) during the investigation, it is essential to save the original source (addressee) of the misleading electronic message sent by the perpetrator(s) and then analyze the email header data. This helps to determine the sender's IP address, which must be checked to see if it is connected to the TOR⁴¹ network or to a VPS or VPN service⁴², the exact time the message was sent and received, the SMTP servers used by the sender and recipient and if the message has an attachment (e.g., a PDF file), what metadata it contains. If the message came from an IP address that can be linked to a subscriber, a request must be sent to the service provider managing the IP address to obtain the subscriber's data. In most cases, the service provider managing the IP address can be checked on public and free online platforms (e.g., whois.domaintools.com). Subsequently, data collection must be carried out in relation to the persons registered at the service address. If the IP address is used by multiple subscribers, all available data must be obtained, and then a narrowing search should be performed. This investigation must be carried out for all IP addresses that can be linked to the perpetrator or the act.
- In parallel with the analysis of technical data, it is advisable to interview persons who have been in contact with the perpetrator (e.g., who received an email or phone call) regarding circumstances that may help identify the perpetrator (e.g., in the case of a phone call: language, accent, gender, tone of voice, manner of expression). During the interview, other

⁴⁰Requests sent in parallel, mainly through international police cooperation channels, result in duplication in processing and, in the vast majority of cases, do not lead to the seizure of funds within a short period of time. In the countries requested, a court order is usually required to seize the money, and judicial authorization is also required to obtain bank data. The ILECC International Information Department has therefore drawn the attention of the investigating authorities to the fact that if the primary objective is to obtain evidence or ensure confiscation, EIO should be used.

⁴¹ The purpose of the TOR network is to encrypt user traffic and hide its source. Data traffic within the network is encrypted and takes place through a chain of interconnected computers, within which a given computer can only see the one computer in front of it and the one behind it, so the device behind the IP addresses recorded during the attack does not have information about the actual sender, meaning that it is not possible to identify the perpetrator based on the IP address.

⁴² In this case, you should contact your VPN or VPS provider to find out whether they store data related to your IP address.

technical data (e.g., phone number) and practices related to transfers/payments, as well as the financial transaction rights of each person, should be clarified.

- Based on the cash flow data obtained, data collection must be carried out on all persons (or business entities) who can be linked to the account or the transaction in question. This may include: the person who initiated the account opening (or who was present⁴³ with that person at the time in the bank branch), the co-cardholder, the legal representative, the senior officer, and the delivery agent.

With regard to the notification telephone number provided to the financial institution, a request for data must be made to the relevant mobile service provider to obtain subscriber data, call logs, cell information, SIM cards associated with the calling number, and subscriber data, call logs, and cell information associated with these SIM cards. Subsequently, the address provided must be verified and a search must be carried out as a coercive measure.

- It may also be justified to contact the Asset Recovery Office of the National Bureau of Investigation of the Riot Police (hereinafter: ARO) in order to verify any other data that may arise in the case and to map the assets derived from the crime. The asset recovery offices of the European Union, the Camden Asset Recovery Inter-Agency Network (CARIN) and the countries that have joined regional organizations modeled on it, through the ARO, can in many cases effectively support the tracking of amounts derived from fraud and the recovery of damages. In order to explore the possibilities, it is advisable to consult with the ARO in advance.
- Based on a text search in criminal case processing databases, background research must not be omitted during the investigation. A beneficiary's bank account number may also be involved in other domestic criminal proceedings, in which case substantive information may already be available regarding the account and the perpetrators, and further connections may also be uncovered. The search must be extended to the TakarNet Land Registry Information System, the domestic and international company information system, the personal and address register, the vehicle registry, the registry of member state judgments, the wanted persons registry, the criminal registry, and the weapons registry.
- If, following the imposition of coercive measures restricting property rights abroad, the property is not transferred within a short period of time, it is advisable to find out whether the domestic law enforcement

⁴³ The seizure of camera recordings made at the bank branch is definitely justified.

authorities expect to receive information at regular intervals regarding the need to maintain the coercive measures.

- If the perpetrator has opened a bank account using a false ID card in the name of another existing person or a photo ID card created with the details of a non-existent person, to establish their identity, the photo on the ID card used to open the account or, if available, a photo of sufficient quality taken at the time of opening the account at the bank branch (or during a cash withdrawal from an ATM), these must be uploaded to the facial recognition system. If the facial recognition system returns a match for a person from a country neighboring Hungary, a request must be sent to the competent Liaison Office to verify the data of the person concerned and obtain their photograph. In certain cases, establishing the identity of the perpetrator may also justify sending a request to the Deputy State Secretariat for Registers of the Ministry of the Interior in order to compile a family tree of the suspects.
- With regard to the perpetrators (straw men), a request must be sent to all Hungarian credit institutions to determine whether they have Hungarian bank accounts, and requests must also be sent to Hungarian telecommunications service providers to determine whether they have Hungarian telephone numbers. In addition to the above, the persons concerned must be checked on social networking sites in order to map their circle of relatives and friends. In the case of an identified perpetrator who is reasonably suspected of having committed the crime, it is essential to obtain information about their criminal record. Based on this, the identity of perpetrators and accomplices previously unknown to the investigating authorities may also be revealed.
- Foreign business organizations potentially involved in money laundering must also be checked in foreign company registers. It may also be necessary to send a request via the ILECC channel to foreign partner authorities to check the bank account numbers, natural and legal persons, telephone numbers, IP and e-mail addresses involved in the case. It is also essential to check whether the suspect used money transfer services outside the banking sector (e.g., Western Union, MoneyGram, etc.). If so, these service providers must also be contacted.
- In order to effectively detect crimes, apprehend perpetrators, secure material evidence, and conduct proceedings successfully and in a timely manner, it may be necessary to set up a joint investigation team (JIT) with the relevant foreign law enforcement authorities. To this end, a proposal must be made to the public prosecutor's office supervising the investigation.

5. CONCLUSION

The effectiveness of anti-money laundering measures is currently one of the most important issues in terms of upholding the rule of law, economic stability, and public trust.

In summary, as a result of the significant measures outlined in the action plan adopted following the Moneyval country report, police and prosecutorial practices regarding criminal proceedings initiated on suspicion of money laundering have been established and standardized in Hungary (at least during the investigative phase), and the necessary organizational and human infrastructure has been put in place. As a result of all this, the conduct of criminal proceedings and the implementation of measures to recover damages caused by the crime have become a kind of routine, which also had a positive impact on the duration of proceedings. The amendment to substantive criminal law broadened the scope of criminal activities, thereby making it easier for the authorities to assess such activities. Furthermore, by using the concept of "property" instead of the previous concept of "thing", the criminal law now includes objects of criminal conduct such as electronic money or cryptocurrency within the scope of seizure. Linking money laundering to the value of the criminal offense has also clarified the jurisdictional issues for the authorities involved, furthermore, all preparatory acts have become punishable, not merely the agreement to commit money laundering.

Given the international nature of money laundering, cross-border exchange of criminal intelligence and cooperation are indispensable; without them, effective detection and asset recovery are out of the question.

The primary scene for judicial and law enforcement cooperation consists of various channels, including Europol, Eurojust, Interpol, liaison offices, and joint investigation teams established with the participation of foreign judicial authorities.

The legal and institutional framework for combating money laundering in Hungary now rests on a solid foundation and is suitable for managing money laundering risks. In the future, however, the focus should not primarily be on creating new rules, but rather on making more effective use of existing tools, strengthening and enhancing cooperation between institutions, and improving the practical effectiveness of law enforcement. Only together can these measures ensure that the fight against money laundering not only formally meets international and domestic expectations but also effectively strengthens the rule of law and the integrity of the economy.

The measures outlined above have clearly yielded results: investigative authorities are successfully uncovering an increasing number of crimes, alongside a growing volume of restitution for damages during their proceedings, which gives cause for optimism when planning future actions against this phenomenon.⁴⁴

REFERENCES

BOOKS AND ARTICLES

1. Belovics, E.; Molnár, G.; Sinku, P., *Büntetőjog II., Különös Rész (Criminal Law II., Special Part)*, ed.: Belovics, E., HVG-ORAC, Budapest 2021, p. 827.
2. Földvári, J.; Gál, I. L., *Magyar büntetőjog, Általános Rész (Hungarian Criminal Law, General Part)*, Osiris, Budapest 2024, p. 316.
3. Gál, I. L., ed., *Magyar büntetőjog, Különös Rész (Hungarian Criminal Law, Special Part)*, Osiris, Budapest 2023, p. 511.
4. Gál, I. L., *Dogmatikai problémák a pénzmosás hatályos magyar szabályozásával kapcsolatban (Dogmatic problems related to the current Hungarian regulations on money laundering)*, *Belügyi Szemle*, 71. évfolyam, 2023/5., pp. 741–763.
5. Kóhalmi, L., *A Nemzetközi Bűnügyi Együttműködés (International Criminal Cooperation)*, in *Magyar Büntetőjog Általános Rész (Hungarian Criminal Law General Part)*, ed.: Tóth, M.; Balogh, Á., Osiris, Budapest 2010, pp. 375-386, 376.
6. Ligeti, K., *A Nemzetközi Bűnügyi Együttműködés Általános Feltételei (General Conditions for International Criminal Cooperation)*, in *Az Európai Büntetőjog Kézikönyve (Handbook of European Criminal Law)*, ed.: Kondorosi, F.; Ligeti, K., Magyar Közlöny Lap- és Könyvkiadó, Budapest 2008, pp. 59-85, 76.
7. Pintér, B., *A pénzmosás elleni küzdelem az új magyar büntető törvénykönyvben (Combating Money Laundering in the New Hungarian Criminal Law)*, doktori értekezés (doctoral thesis), Pécsi Tudományegyetem, Pécs 2012, p. 2.

⁴⁴ According to data from the Unified Investigative Authority and Prosecutor's Office Crime Statistics, the investigation success rate ranged between 87.8% and 92.3% between 2020 and 2024, which can be considered extremely good.

LEGAL ACTS

1. Directive (EU) 2018/1673 of the European Parliament and of the Council of 23 October 2018 on combating money laundering by criminal law, OJ L 284 of 12/11/2018.
2. 1996. évi XXXVIII. törvény a nemzetközi bűnügyi jogsegélyről (Act on international legal assistance in criminal matters), Magyar Közlöny 1996/54.
3. 2009. évi LXXXV. törvény a pénzforgalmi szolgáltatás nyújtásáról (Act on the provision of payment services), Magyar Közlöny 2009/100.
4. 2012. évi C. törvény a Büntető Törvénykönyvről (Act on the Criminal Code), Magyar Közlöny 2012/92.
5. 2012. évi CLXXX. törvény az Európai Unió tagállamaival folytatott bűnügyi együttműködésről (Act on criminal cooperation with Member States of the European Union), Magyar Közlöny 2012/160.
6. 2013. évi CCXXXVII. törvény a hitelintézetekről és a pénzügyi vállalkozásokról (Act on Credit Institutions and Financial Enterprises), Magyar Közlöny 2013/217.
7. 2017. évi LIII. törvény a pénzmosás és a terrorizmus finanszírozása megelőzéséről és megakadályozásáról (Act on the prevention and combating of money laundering and terrorist financing), Magyar Közlöny 2017/75.
8. 2017. évi XC. törvény a büntetőeljárásról (Act on Criminal Procedure), Magyar Közlöny 2017/99.
9. 2020. évi XLIII. törvény a büntetőeljárásról szóló törvény és más kapcsolódó törvények módosításáról (Act on amending the Criminal Procedure Act and other related acts), Magyar Közlöny 2020/129.
10. 329/2007. (XII. 13.) Korm. rendelet a Rendőrség szerveiről és a Rendőrség szerveinek feladat- és hatásköréről (Government Decree on the Police and the tasks and powers of the Police), Magyar Közlöny 2007/174.
11. 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről (Minister of the Interior Decree on the powers and jurisdiction of police investigative authorities), Magyar Közlöny 2013/104.
12. 1688/2017. (IX. 22.) Korm. határozat az Európa Tanács Moneyval országjelentésben Magyarország részére megfogalmazott pénzmosás elleni ajánlások végrehajtásáról készített akciótervről (Government Resolution on the action plan for implementing the recommendations against money laundering made to Hungary by the Council of Europe's Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism), Magyar Közlöny 2017/153.
13. 1691/2018. (XII. 17.) Korm. határozat a pénzmosás és terrorizmus finanszírozása elleni nemzeti kockázatértékelés felülvizsgálata

eredményképp megfogalmazott intézkedésekről (Government Resolution on measures formulated as a result of the review of the national risk assessment for money laundering and terrorist financing), Magyar Közlöny 2018/201.

14. 25/2017. (VIII. 17.) ORFK utasítás az Európai Rendőrségi Hivatal által működtetett Európai Biztonságos Hálózat alkalmazásainak felhasználásával megvalósuló együttműködés és információcsere rendjéről szóló 23/2016. (IX. 15.) BM-NGM együttes utasítás végrehajtásáról (Instruction of the National Police Headquarters on the implementation of Joint Instruction 23/2016 (IX. 15.) BM-NGM on the procedure for cooperation and information exchange using the applications of the European Secure Network operated by the European Police Office), Hivatalos Értesítő 2017/40.
15. 20/2018 (V. 31.) ORFK utasítás a bűncselekményekből származó jövedelmek és a bűncselekményekhez kapcsolódó egyéb javak felkutatása, azonosítása és a vagyonsbiztosítás érdekében teendő feladatokról (Instruction of the National Police Headquarters on the search for and identification of income derived from criminal offenses and other assets related to criminal offenses, and on tasks to be performed for the purpose of securing assets), Hivatalos Értesítő 2018/21.
16. 11/2024. (III. 21.) ORFK utasítás a kapcsolattartási szolgálati helyek működéséről (Instruction of the National Police Headquarters on the operation of liaison offices), Hivatalos Értesítő 2024/16.
17. Circular of Department of Priority and Military Cases of the Hungarian Prosecutor General's Office No. KF.9725/2004/379-II, No. TPK.1008/2017/37-I. and No. TPK.1008/2017/37-II.
18. Information note for the purpose of informing members of parliament, Office of the National Assembly, Public Collections and Public Education Directorate, Representative Information Service 2025/18 (May 30, 2025).

COURT PRACTICE

1. Hungarian Supreme Court decision No. BH 2019.125.

NETWORK RESOURCES

1. <https://www.police.hu/hu/a-rendorsegrol/testulet/teruleti-szervek/nemzetkozi-bunugyi-egyuttmukodesi-kozpont>, 8 January, 2026.

2. <https://www.mnb.hu/felugyelet/szabalyozas/penzmosas-ellen/korlatozo-intezkedesek-szankciok/penzugyi-akciocsoport-fatf>, 14 January, 2026.