GIS Odyssey Journal

2026 • Volume 6 • Number 2

https://doi.org/10.57599/gisoj.2026.6.2.205

Agnieszka Gryszczyńska[1]

THE GEOGRAPHY OF IMPUNITY – THE CHALLENGES OF CROSS-BORDER CRIMINAL PROCEEDINGS IN INVESTMENT FRAUD CASES

Abstract: For those who commit crimes in cyberspace, cross-border activity is not problematic; rather, it serves as an effective method for maintaining anonymity and evading criminal liability. For law enforcement agencies, the cross-border nature of cybercrime poses a significant regulatory, operational and technical challenge. The gathering of electronic evidence, the execution of investigative inquiries and the undertaking of procedural actions, including but not limited to interrogations, searches, and arrests, necessitate collaboration with law enforcement agencies, judicial authorities and service providers across multiple jurisdictions. This collaboration is facilitated by the application of a range of international cooperation instruments. The analysis of the cross-border challenges confronting law enforcement agencies was predicated on the *modus operandi* of the perpetrators behind fraudulent investment platforms, the algorithm necessary for law enforcement agencies to initiate action, and an examination of the fundamental regulations governing cooperation in criminal proceedings involving activities in cyberspace. The activities of groups setting up fraudulent investment platforms and encouraging people to invest are on the rise, both in Poland and globally. This also highlights regulatory loopholes and reveals the geography of impunity – that is, areas where criminal networks are based, and where instruments of international cooperation in criminal matters have limited effectiveness.

Keywords: cybersecurity, cybercrime, cyberspace, fraud, investment fraud, jurisdiction, e-evidence

Received: 10 August 2026; accepted: 27 August 2026; revised: 6 September 2026

[1] Cardinal Stefan Wyszyński University in Warsaw, Faculty of Law and Administration, Department of Informatics Law, ORCID ID: 0000-0003-3004-5253, email: a.gryszczynska@uksw.edu.pl

Introduction

The number of security incidents and crimes that can collectively be described as investment fraud has been rising in recent years. The CERT Polska team has identified investment fraud as the most financially damaging threat to Polish cyberspace in 2025 (CERT, 2026). Similarly, the CSIRT KNF (a sectoral CSIRT established by the Polish Financial Supervision Authority) has identified investment fraud as the most prevalent and damaging attack scenario aimed at financial theft (CSIRT KNF, 2026). The number of victims of this type of activity and the financial losses – both overall and on an individual basis – that is, those incurred by individual victims – are significant. The activities of groups establishing fraudulent investment platforms and encouraging investment can also have a detrimental effect on the level of public trust in the financial market, investment institutions and state regulatory bodies, and impose a significant burden on law enforcement agencies and the courts. Consequently, the present study will analyse in detail the scenario of investment fraud in which perpetrators set up fake investment platform websites, which they then extensively promote on mainstream websites, search engines and social media.

While the article focuses on examples of groups operating to the disadvantage of Polish citizens, it is important to note that investment fraud is a transnational issue, with criminal call centres experiencing significant growth in Southeast Asia. These centres target citizens of various countries, including China, the United States, and Canada (U.S. Department of Justice, 2025; Competition Bureau, 2026).

The cross-border and organised nature of the perpetrators' activities, their use of anonymisation tools and modern technologies – including artificial intelligence – mean that combating this type of crime is challenging and requires transnational cooperation between law enforcement and judicial authorities, other public institutions, entities in the financial sector and providers of electronic services.

The success of such efforts, namely the identification of the perpetrators and their subsequent apprehension and prosecution, is determined by a multitude of factors. In order to identify the determinants of an effective criminal law response to investment fraud, this analysis examines the *modus operandi* of perpetrators and the basic framework necessary for law enforcement agencies to take action in such cases. In light of the distinct characteristics inherent to such legal proceedings, the analysis encompassed a comprehensive evaluation of the legal provisions pertaining to the preservation of data and electronic evidence for the proceedings from entities situated across various jurisdictions. This analysis also encompassed the conduct of proceedings through international legal assistance, with the objective of assessing their applicability and effectiveness.

Analysis of the state of the problems

A meticulous examination of incident reports published by both public and private entities, encompassing both international and national scope, reveals a persistent and escalating trend in cyber threats. In Poland, the 2024 report by the Government

Plenipotentiary for Cybersecurity indicates that national-level CSIRT teams recorded a total of 111,660 ICT security incidents (Plenipotentiary's Report, 2024). In 2025, the total number of incidents nationwide increased at an unprecedented rate. According to the report by the Government Plenipotentiary for Cybersecurity for 2025, national-level CSIRT teams recorded a total of 272,941 ICT security incidents. Of these, the CSIRT NASK (Computer Security Incident Response Team, as defined in Article 2(3) of the Act of 5 July 2018 on the National Cybersecurity System) recorded 260,783 incidents (representing an increase of 152 % compared with 2024), CSIRT GOV recorded 5,033 incidents (representing a 26 % increase compared with 2024), and CSIRT MON recorded 7,125 incidents (representing a 68.9 % increase compared with 2024) (Report of the Plenipotentiary, 2025).

Among the incidents recorded by the CSIRT NASK, those classified as computer fraud predominate, accounting for 97 % of all incidents handled (CERT, 2026). Furthermore, data provided by the National Bank of Poland (NBP) indicates that the primary objective of the perpetrators is to monetise. In its report for the first quarter of 2026, the NBP observed that the number of fraudulent transactions involving non-cash payment instruments (i.e. payment cards, bank transfers and direct debits) had increased by 3.4% compared with the fourth quarter of 2025, while the value of such transactions was 46.8% higher (NBP, 2026). This is linked to a significant rise in the value of fraud in the category of transactions involving bank transfers. A thorough examination of data pertaining to incidents within this category further suggests that the number of incidents associated with the operations of fraudulent investment platforms is increasing.

According to a report by CERT Polska, investment fraud constituted the most prevalent category of phishing attacks in 2025. In 2025, the number of domains linked to fraudulent investments that were added to the Warning List increased to 98,663, in comparison to 43,172 domains in the previous year. This represents 40 % of all domains deemed malicious by CSIRT NASK and added to the Warning List (the Warning List is a publicly available list of internet domains used for data theft and the misappropriation of internet users' assets, maintained by CSIRT NASK pursuant to the ACAEC, 2023). Furthermore, of the 41,751 dangerous domains identified and reported for blocking by CSIRT KNF in 2025, 96.34% were linked to fraudulent investment schemes (CSIRT KNF, 2026).

The increase in activity by perpetrators responsible for creating fake investment platform websites is also evident in the statistics of Polish law enforcement agencies, although it is not possible to provide clear and consistent data due to differences in how cases are described in the IT systems of the public prosecutor's office and the police. In the majority of cases, proceedings concerning fraudulent investments are classified as fraud, i.e. offences under Article 286 § 1 of the Polish Penal Code (PCC, 1997). However, it is not always possible, based on the description of the offence, to unequivocally determine the mechanism of the fraud or whether it was committed in connection with a fraudulent investment platform.

The creation of the 'investment platforms' coordination category – utilised to flag criminal proceedings in the public prosecutor's office IT system – was intended to provide

analytical data for the study of cybercrime trends in Poland and to enhance the coordination of cases in this area. However, the obligation to manually assign proceedings to this coordination category is not always fulfilled, and the data on the number of cases involving investment fraud is incomplete; nevertheless, an increased trend can be observed on the basis of this data.

As demonstrated in Chart 1, the number of cases concerning fraudulent investment platforms registered with the Public Prosecutor's Office in Poland is rising. However, it must be noted that the statistical number of cases does not fully reflect the scale of the phenomenon, as a single case may cover one or multiple investment platforms operated by the same organised criminal group. Consequently, a single criminal case may involve anywhere from a few to several thousand victims and from a few to several dozen perpetrators. The methodologies developed in Poland for conducting proceedings involving multiple victims, in conjunction with the public prosecutor's office's central information system, facilitates the reduction of the number of cases registered by enabling the swift identification of proceedings that have already been initiated and the addition of reports filed by subsequent victims to them.

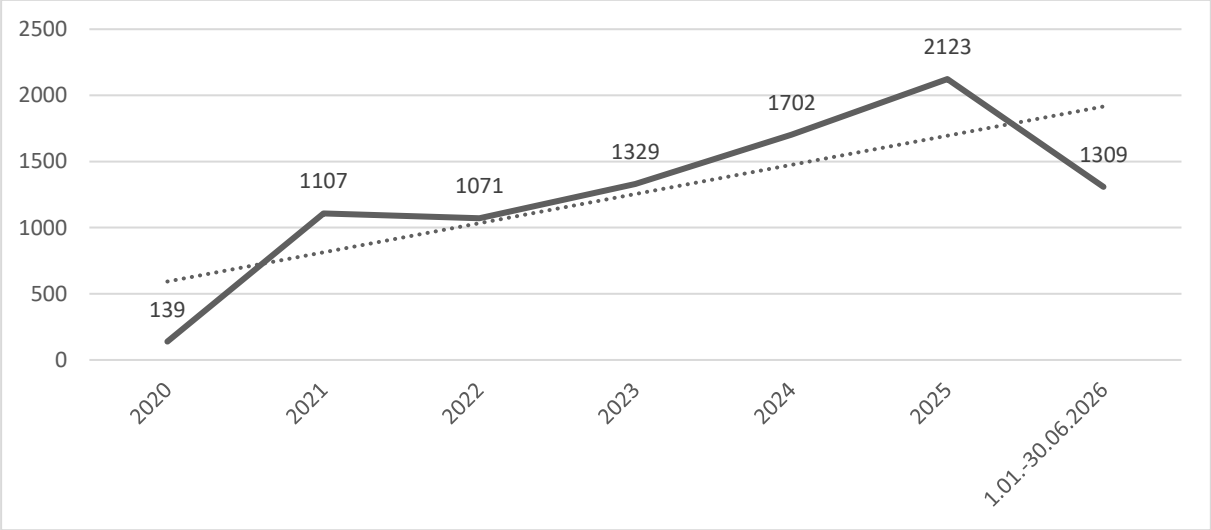

Chart 1. Number of registered cases categorised under ‘investment platforms’ for coordination purposes in Poland
Source: Author’s own analysis of statistical data from the Public Prosecutor’s Office’s IT system, as at 30 June 2026

Crimes committed via fraudulent investment platforms vary in nature, and the perpetrators' methods may differ from classic deception aimed at inducing another person to dispose of their property to their detriment. A number of these offences encompass, for instance, the installation of remote desktop software on victims' devices, the acquisition of victims' online banking login credentials, and the perpetration of identity theft.

Irrespective of the subsequent steps taken to obtain funds from the victims, the first stage involves the perpetrators creating websites that mimic those of an investment

platform. These sites are extensively promoted on prominent websites, social media platforms and via search engine results. The advertisements for a given platform highlight the potential returns on investment. The promotional materials and the platform's website both make use of specialist economic and financial terminology, the purpose of which is to inspire trust and create a professional image of an investment market entity. It is imperative to note that, from the outset of the advertising stage, victims are misled with regard to the entity operating the investment platform or the nature of the investment. It is important to emphasise that the model under scrutiny does not encompass the provision of financial instruments. The perpetrators accept funds from victims, which are then not invested, but merely transferred between various bank accounts and converted into crypto-assets, ultimately ending up with those responsible for organising the criminal activity. The dissemination of investment platforms has been facilitated by social media, with promotions occurring through two primary channels: firstly, through the hacking of accounts belonging to ordinary users, with the intention of providing a semblance of credibility to the posts amongst their acquaintances; and secondly, through the creation of accounts specifically designed to promote fictitious investment platforms, known as bot accounts. It is evident that these accounts are utilised for the purpose of enhancing the reach through the dissemination of content or engagement with the material in a variety of forms.

The fraudulent investment scheme is not confined to any specific geographical region. It is evident that organised criminal groups engage in this type of activity in a multitude of countries, often in a simultaneous manner. At various times, the perpetrators have explored different social engineering tactics aimed at persuading potential investors to make payments – ranging from investing in crypto-assets and company shares to investments in artificial intelligence and investments where decisions on what to invest in are made by artificial intelligence. However, it is important to note that the advertisements and themes encouraging investment are tailored to local contexts and significant political, economic or social events. In the context of Poland, the presidential election provided a case study in the exploitation of current events. Following the announcement of the results, a series of advertisements emerged, purportedly implicating the president in a scandal. This mechanism is predicated on the exploitation of heightened public attention and the emotional engagement of the audience. Simultaneously, an analysis of the advertising accounts indicated that a single account is utilised for the dissemination of advertisements in various languages and with different script variations tailored to specific markets. This finding confirms the international reach of the groups responsible for these fraudulent investments (Ślusarek & Lange, 2026).

Since 2023, there has been an increase in criminal activity related to the creation of manipulated video material, otherwise known as deep fakes. According to Article 3(60) of the Regulation 2024/1689, deep fake is defined as AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful. The deployment of deep fakes in investment fraud schemes is a contemporary phenomenon, attributable to their efficacy in social engineering. The manipulated recordings lead the victim to believe that

the investment is legitimate and profitable, due to the trust inspired in the victims by the person the perpetrators are impersonating – a politician, sportsman, businessman or celebrity who has themselves achieved financial success. In doing so, the perpetrators exploit one of the universal principles of influence identified by Robert Cialdini – the principle of authority (Cialdini, 2001).

The advertisements direct the unsuspecting individual to simple landing pages, where, in addition to the investment offer itself, there is a contact form. This form requires the victim to provide personal details, including their full name, email address and telephone number, so that a representative of the investment platform can contact them later (the second stage of the perpetrators' scheme). No further information is required on these type of pages. The collection of rudimentary contact information by these perpetrators is sufficient to facilitate the progression of their operations without provoking the victim's suspicion.

The third key stage of the perpetrators' operation is direct contact with the victim. The individuals referred to as 'telemarketers' – who self-identify as 'consultants', 'brokers' or 'client advisors' – actively engage in the process of persuading the victim to invest. These individuals call the 'investor' to present an offer. They help the victim set up a personal account on a fraudulent investment platform through which the client is supposed to carry out transactions. Within the account settings, the victim is able to verify the present balance of their alleged investments or the values of derivatives, thereby fostering increased confidence.

In addition to the initial tactic of persuading the victim to transfer funds directly to the specified bank account, those engaged in criminal activity employ a variety of other methods to obtain funds from the victim as part of the fraudulent investment scheme. The most prevalent of these is the persuasion of the victim to install a remote desktop application (e.g. TeamViewer, AnyDesk or UltraViewer), which enables the perpetrators to take control of the victim's device and obtain full access to the login credentials utilised for online banking.

In certain instances, a representative of the platform offering the fraudulent investment scheme requested that the 'investor' partake in a claimed verification process as a component of Anti-Money Laundering (AML) procedures. In order to proceed with the investment process, the investor is instructed to navigate to a designated webpage and submit their precise personal information, along with a scanned copy of their identification documentation. It has been established that this scheme encompasses the illicit acquisition of online banking login credentials through the utilisation of a fraudulent website that closely resembles the legitimate online banking login page.

Initially, the victim is persuaded to invest a relatively small amount – ranging from 100 to 500 euros. Subsequent to a period of several days, the call centre operators inform the investors of the success of the investment and the multiplication of the initial investment amount, thereby encouraging them to invest significantly larger sums of money. Perpetrators invest significant time and effort in establishing a relationship of trust with their victims. This is achieved by offering assistance and guidance, thereby assuming the role of a credible expert. At this juncture, should the victim wish to withdraw

the funds they have paid in and receive a return on their investment, these funds are transferred to their own bank account. However, in the majority of cases, the funds are transferred from an account belonging to another victim. In such cases, the perpetrators provide one victim with a bank account belonging to another victim. In this manner, funds are extracted from one individual, while the other receives a transfer that is intended to create the impression of a return on investment. This is designed to instil trust and persuade the victim to invest significantly larger sums.

The utilisation of minimal financial resources within the victims' accounts enables the perpetrators to circumvent the detection of the accounts used to receive and launder substantial sums of money. Furthermore, this process serves to considerably complicate the subsequent identification of the accounts of so-called 'money mules'.

On certain technologically sophisticated platforms, users have the option of utilising 'demo' accounts, which allow them to track the projected growth of their investments. Subsequently, the investors are convinced that they will make a profit, and payments are made into accounts provided by the individuals encouraging them to invest, or indicated on the platform's website on their customer profile. Furthermore, the value of the investment portfolio is purportedly increased, and the investor is able to observe this development on the platform. However, the observed growth was not indicative of actual financial performance, as the funds in question were not being invested. Consequently, the charts depicting an increase in the value of these funds were the result of artificial manipulation. The trust established in this manner enabled the perpetrators to persuade their victims to invest larger sums. In numerous instances, the victims also utilised the additional funds obtained through loans or borrowing from family or friends (Gryszczyńska, 2024).

The losses suffered by victims are closely linked to the investment fraud scenario, the involvement of the perpetrators, the tailoring of social engineering techniques to the client's profile, the victim's level of technical knowledge and adherence to digital hygiene, and the level of trust the 'investor' placed in the representative of the investment platform. It is a commonly held view that investment frauds typically result in significant financial losses for their victims. A victim who has been manipulated by the perpetrators is convinced that the investment will generate a high profit, and as a result, frequently begins to behave irrationally.

In scenarios based on the classic fraud, the victims themselves made transfers to accounts specified by the perpetrators. Subsequent payments were coerced through the use of social engineering, whereby victims were deceived into withdrawing their funds by informing them of penalties or charges relating to excessive profits or necessary tax payments.

In scenarios where remote access software had been installed on the victim's computer, the perpetrators gained access to the victim's online banking credentials and proceeded to carry out transfers themselves. As the victims later reported, they installed remote desktop software so that a 'consultant' could assist them in investing or opening accounts on cryptocurrency exchanges.

It was established that some of the victims were subjected to repeated deception, resulting in unfavourable financial transactions, perpetrated by a single organised group. Another fraudulent scheme that has been observed involves the impersonation of a law firm, with the objective of offering paid assistance in the recovery of funds that have been misplaced.

Material and method

As demonstrated by the simplified scenario outlined above, investment fraud perpetrated through the use of fraudulent platform websites is the domain of organised criminal groups characterised by a distinct division of roles. This encompasses a wide range of responsibilities, including but not limited to: the creation of advertising materials and websites; the acquisition of contact details; the facilitation of interactions with victims; and the management of financial transactions. This organisational structure facilitates the execution of operations on a large scale, while concomitantly hindering the identification of the perpetrators.

Within criminal organisations, three key teams can be identified: lead teams, whose task is to obtain the contact details of potential victims; call centre teams, whose task is to make direct contact with victims and carry out further manipulation; and teams responsible for obtaining money mules' accounts and money laundering. These teams may operate within a single organised criminal group. There are also increasing indications of the development of the Crime-as-a-Service (CaaS) model, under which individual elements of the attackers' infrastructure are offered as services by other criminal groups.

The structure of selected groups and the scope of their activities can already be determined on the basis of OSINT analyses and findings from several major criminal proceedings conducted in Poland.

Presently, the most extensive investigation into fraudulent investment schemes is being conducted by the Regional Public Prosecutor's Office in Kraków. This investigation encompasses five interconnected investment platforms that purported to offer investment opportunities on the over-the-counter FOREX market. A total of approximately 2,000 victims have been identified, from whom a total of around 80,000,000 PLN was the subject of fraud (PRK, 2025). During the investigation in 2025, more than a dozen people were arrested, whilst in 2026, officers from the Central Bureau for Combating Cybercrime (CBZC), together with representatives of the National Police of Ukraine, uncovered three operational call centres in Ukraine, where a number of computers, servers, mobile phones and data storage devices were seized. In addition, staff members employed in call centres were subjects of inquiry (CBZC, 2026). The case remains ongoing.

As part of an investigation by the Regional Public Prosecutor's Office in Łódź, officers from the Central Bureau for Combating Cybercrime, in cooperation with the Cyberpolice Department of the National Police of Ukraine, successfully dismantled an organised

criminal group responsible for large-scale investment fraud and arrested six main suspects (CBZC, 2025).

As part of an investigation by the Regional Public Prosecutor's Office in Rzeszów, the CBZC, in collaboration with the Economic Security Bureau of Ukraine, has closed one of the call centres in Kharkiv (CBZC, 2024).

Results

The investigations revealed that the groups responsible for offences committed using fraudulent investment platforms were led by foreign nationals, the call centres were located in Ukraine, and the victims were from various countries, including Poland. The group under investigation by the Regional Public Prosecutor's Office in Kraków demonstrated a remarkably elevated degree of organisation, evincing characteristics comparable to those of a corporation. It possessed specialised organisational units, including a human resources department, an information technology department, and separate departments designated for Russian-speaking, English-speaking, Italian-speaking, and Spanish-speaking 'clients'. Notably, the group also comprised four distinct departments dedicated to serving Polish-speaking 'clients'. The members of the group who were posing as representatives of the aforementioned platforms proceeded to introduce themselves to their victims in Poland. They used false, Polish-sounding first names and surnames in the process. These members operated from call centres located in three Ukrainian cities via investment platforms that were professionally run and administered.

From a broader perspective, it should be noted that the structure and mode of operation of individual groups – and even the call centre model itself – are by no means uniform. Call centres located in Ukraine, which employ dedicated teams of Polish-speaking workers, rely on paid and voluntary work carried out by call centre agents recruited via the internet or instant messaging platforms e.g. Telegram (Klimczuk, 2026.). Call centres located in Southeast Asia operate on entirely different principles; they rely mainly on unpaid, forced labour carried out by people confined to so-called scam compounds and physically punished for failing to meet the financial targets set by their group leaders (Lazarus, Chiang, Button, 2026). The United Nations estimates that more than 300,000 people have been trafficked into Southeast Asian scam compounds (Griffiths, 2026).

Discussion

The effectiveness of law enforcement agencies in cases involving fraudulent investment platforms depends on a number of factors. An effective criminal justice response to offences committed in cyberspace is dependent on several key factors, including the speed of the response, the effective management of law enforcement agencies' information resources, the organisation of the agencies responsible for responding to cybercrime, and regulatory frameworks (Gryszczyńska, 2025). Based on an analysis of proceedings conducted in Poland, it can be seen that the time within which law

enforcement agencies are informed of a cybercrime is crucial, as is the scope of data that can be obtained from the victim, indicating the infrastructure used by the perpetrators, as well as bank accounts or accounts on cryptocurrency exchanges. Cases involving the arrest of perpetrators responsible for investment fraud were usually handled by prosecutors specialising in cybercrime and police officers from the Central Bureau for Combating Cybercrime. Specialised investigators can gather useful information for the proceedings as early as the victim's first interview. Furthermore, when officers specialising in combating cybercrime conduct the investigation, they immediately examine and analyse the victim's computers or other devices containing data and electronic evidence (particularly if the perpetrators have installed remote desktop software on the victim's device). This allows for a more focused investigation and enables further analysis. It is essential to secure data relating to money transfers without delay, including recipient accounts and login details for clients' accounts and cryptocurrency exchange accounts, which the perpetrators usually set up and manage using the victim's data. If the service provider is based in the country where the legal proceedings are taking place, the data can be obtained within a timeframe ranging from a few days to several weeks. However, it is relatively rare for perpetrators to use infrastructure from the country where the victim is affected. Even at this stage, it is usually necessary to approach various service providers using the appropriate instruments of international cooperation.

The most appropriate instruments for international cooperation depend on several factors. The most important factor is the location of the relevant entity. If the entity requesting the data is a law enforcement or judicial authority within the EU and the data provider is also established in the EU, obtaining the data is relatively quick and straightforward using instruments of international cooperation within the EU. This is particularly thanks to the introduction of the European Investigation Order (Directive 2014/41/EU) in 2017. However, it should be noted that the EIO is not applicable in Denmark or Ireland - home to major service providers. The standard method for submitting requests for access to data is mutual legal assistance (MLA). However, this is a slow and complicated process requiring the use of diplomatic channels alongside penal proceedings. Obtaining data from service providers outside the EU, particularly in the United States, takes an average of over a year. For this reason, law enforcement agencies are increasingly relying on voluntary cooperation with service providers to obtain non-content data.

Following many years of negotiations, in 2023 the European Union adopted a new regulation on electronic evidence. This introduces a new model of mutual recognition to ensure cross-border access to data for criminal proceedings (Regulation 2023/1543 and Directive (EU) 2023/1544). The new regulation aims to provide a more efficient way of obtaining data from service providers operating within the EU but outside the state conducting the proceedings. It enables data to be requested directly from service providers, bypassing the authorities in the relevant Member State. Service providers will be required to designate at least one establishment or representative authorised to receive orders for the production of electronic evidence, and respond efficiently to such orders. Alongside the introduction of the European Order for the Production of Electronic

Evidence (EPOC) and the European Preservation Order for Electronic Evidence (EPOC-PR), the EU is developing a secure online portal to handle electronic requests and responses, as well as related procedures. The e-Evidence Digital Exchange System (e-EDES) aims to reduce the time and costs involved in transmitting requests such as EIOs, EPOCs and EPOC-PRs, as well as evidence.

While the adoption of the e-Evidence package is an important step towards resolving the issue of access to data for criminal proceedings, its effectiveness and practical application depend on several issues that the package leaves to the Member States' discretion or omits it altogether. It also depends on reaching an agreement with the United States (Tosza, 2024).

However, this regulation does not solve many of the practical problems encountered when investigating investment fraud. Even if data relevant to establishing the identity of the perpetrators is successfully obtained during the investigation using instruments for cooperation in criminal matters within the EU, subsequent steps require recourse to international conventions or bilateral agreements. In the aforementioned case handled by the Regional Public Prosecutor's Office in Kraków, the contents of a server used to set up and administer the websites of fraudulent investment platforms were seized following the execution of the European Investigation Order by the German public prosecutor's office. This subsequently made it possible to identify the location of criminal call centres in Ukraine (PRK, 2025). Subsequent actions therefore had to be based on other instruments of international cooperation.

Depending on the nature of the offence, the country involved, the scope of the required data, or the need for cooperation in criminal matters, it is necessary to apply international conventions and agreements relating to such cooperation.

In cases involving cybercrime, the Council of Europe's Convention on Cybercrime (CETS No. 185), to which 82 countries have already acceded, is an effective means of preserving digital data without delay. The Second Additional Protocol (2022) is intended to provide broader possibilities for obtaining data directly from data providers; however, it has not yet entered into force, due to the lack of at least five ratifications. Similarly, the UN Convention against Cybercrime (2024) has not yet entered into force. However, the applicability of conventions on cybercrime will depend on the perpetrators' *modus operandi*. If the only offence committed is traditional fraud, the Council of Europe's Convention on Cybercrime will not apply. If the perpetrators gain access to the victim's device via remote desktop software, the act committed undoubtedly constitutes an offence classified as a cybercrime under the Convention.

Given that organised criminal groups of an international nature are behind the scheme of fraudulent investment scams, the United Nations Convention against Transnational Organised Crime (UNTOC, 2000), ratified by 194 countries, will apply.

Regardless of the established foundations for international cooperation in cases involving fraudulent investment platforms, it should be noted that many proceedings are hindered by entities that refuse to cooperate and knowingly provide services to other criminals ('bulletproof hosting providers'), or by countries that fail to cooperate in executing requests for mutual legal assistance. Furthermore, criminal operations are

often located in regions affected by armed conflict, where the rule of law is challenged and illicit economies thrive. These conditions offer greater protection from detection and interdiction. Examples include war-torn Ukraine, Mexican states dominated by drug cartels, and corruption-ridden African economies (Griffiths, 2026).

Researchers describing human trafficking linked to scam compounds in Southeast Asia point out that "scam compounds function as industrialised socio-technical systems embedded within licit - illicit economies, exploiting digital infrastructures, deregulated Special Economic Zones, and migration precarity" (Lazarus, Chiang, Dimitrova, Thu, & Essien, 2026). They also note that many of these compounds are located in Special Economic Zones (SEZs), which are areas designed to attract foreign investment where normal legal safeguards are suspended and local authorities receive monthly payments from the owners of these criminal compounds (Lazarus, 2026). The links between local structures and criminal activity, or the assumption that such activity forms part of a country's economy, undoubtedly contribute to the lack of effective responses to requests for legal assistance in criminal matters. In addition to the problem of the 'geography of impunity', shortcomings in the corporate accountability of digital and financial service providers are also highlighted.

Conclusions

The research presented confirms that investment fraud remains the most common type of cybercrime, targeting participants in the financial market. The main tools used to recruit victims are fake websites and advertisements employing social engineering techniques. These criminal schemes are orchestrated by organised criminal groups with structures resembling large corporations and an international reach.

Gathering and preserving the necessary data and evidence, analysing it to identify and apprehend the perpetrators, and recovering assets derived from criminal activity requires immediate action, taken with a sense of urgency, to promptly identify and preserve further data necessary for criminal proceedings. Time is a critical factor in these operations. Due to the short retention periods for telecommunications data, which vary from country to country, and the lack of internet data retention, law enforcement agencies can only achieve investigative success by obtaining data immediately after an incident and tracking the perpetrator in near real time. This is not always possible using the available instruments of international cooperation in criminal matters. While voluntary forms of cooperation are usually the quickest, they are not always available or feasible.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

Declaration of Competing Interests

The author declares that she has no known competing financial interests or personal relationships that could have appeared to influence the work reported in this pape.

Data Availability

Publicly accessible data, including research papers listed in the references.

Use of Generative AI and AI-Assisted Technologies

No generative AI or AI-assisted technologies were employed in the preparation of this manuscript.

References

ACAEC (2023). Act of 28 July 2023 on Combating Abuse in Electronic Communications. Journal of Laws 2024, item 1803, as amended.

CBZC (2024). International cooperation between the CBZC and Ukrainian law enforcement agencies has led to the dismantling of the infrastructure of fraudulent investment platforms in Kharkiv. https://cbzc.policja.gov.pl/bzc/aktualnosci/388,Miedzynarodowa-wspolpraca-CBZC-z-organami-scigania-Ukrainy-pozwolila-na-likwidac.html?search=61318 [access: 9.08.2026].

CBZC (2025). Success of an international operation against investment fraudsters! https://cbzc.policja.gov.pl/bzc/aktualnosci/509,Sukces-miedzynarodowej-operacji-przeciwko-oszustom-inwestycyjnym.html?search=61318 [access: 9.08.2026].

CBZC (2026). Losses amounting to 80 million zlotys – three call centres shut down in Ukraine. https://cbzc.policja.gov.pl/bzc/aktualnosci/951,Straty-siegajace-80-mln-zlotych-3-call-center-rozbite-na-terenie-Ukrainy.html [access: 9.08.2026].

CERT (2025). CERT Polska's 2025 Annual Report. The security landscape of the Polish internet. CERT Polska. 2026. https://cert.pl/uploads/docs/Raport_CP_2025.pdf [access: 9.08.2026].

Cialdini R.B. (2001). Influence: Science and Practice. Allyn & Bacon, 2001.

Competition Bureau (2026). Fraud Prevention Month to bring hidden crime into the spotlight. https://www.canada.ca/en/competition-bureau/news/2026/03/fraud-prevention-month-to-bring-hidden-crime-into-the-spotlight.html [access: 9.08.2026].

CSIRT KNF. 2026. Annual Cybersecurity Report. KNF (2026). https://www.knf.gov.pl/dla_rynku/CSIRT_KNF/Raport_Roczny_Cyberbezpieczenstwa [access: 9.08.2026].

Klimczuk O. (2026). Ukrainian police have shut down 94 fraudulent call centres. Cyberdefence24. https://cyberdefence24.pl/armia-i-sluzby/wojna-w-ukrainie/ukrainska-policja-zamknela-94-oszukancze-call-center [access: 9.08.2026].

Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters, OJ L 130, 1.5.2014, pp. 1–36.

Directive 2023/1544 of the European Parliament and of the Council of 12 July 2023 laying down harmonised rules on the designation of designated establishments and the appointment of legal representatives for the purpose of gathering electronic evidence in criminal proceedings. OJ L 191, 28.7.2023, pp. 181–190.

Griffiths J. (2026). Dial S for scam. How criminal call centres spread from Southeast Asia to become a global crisis. The Globe and Mail 5.8.2026. https://www.theglobeandmail.com/world/article-scam-call-centres-southeast-asia-global-crisis-organized-crime/ [access: 9.08.2026].

Gryszczyńska A. (2024). The use of artificial intelligence in investment fraud; Cybersecurity vs. artificial intelligence. In: B. Szafrański (ed.). Law, Computer Science and Management. The Military University of Technology Publishing House. Warszawa, pp. 135–152.

Gryszczyńska A. (2025). Factors determining an effective criminal law response to cyber threats. In: A. Gryszczyńska, G. Szpor, W.R. Wiewiórowski (ed.). Internet. Cyber resilience. C.H. Beck. Warsaw, pp. 39–56.

Lazarus S. (2026). Inside Southeast Asia's industrialised fraud factories. https://blogs.lse.ac.uk/businessreview/2026/02/12/inside-southeast-asias-industrialised-fraud-factories/ [access: 9.08.2026].

Lazarus S., Chiang M., Button M. 2026. Assessing Human Trafficking and Cybercrime Intersections Through Survivor Narratives. Deviant Behavior, 47 (7), pp. 1252–1269. https://doi.org/10.1080/01639625.2025.2470402.

Lazarus S., Chiang M., Dimitrova R.S., Thu T.T., Essien E. (2026). What Do We Know About Human Trafficking and Scam Compounds in Southeast Asia (2020–2025)? A Qualitative Meta-Synthesis of Coercive Deviant Enterprises. Deviant Behavior, 47(6), pp. 1091–1123. https://doi.org/10.1080/01639625.2025.2604138.

NBP (2026). Information on fraudulent transactions carried out using non-cash payment instruments in the first quarter of 2026. National Bank of Poland. https://nbp.pl/wp-content/uploads/2026/07/Informacja-o-transakcjach-oszukanczych-w-I-kwartale-2026.pdf [access: 9.08.2026].

NCS (2018). The Act of 5 July 2018 on the National Cybersecurity System. Journal of Laws of 2026, item 20, as amended.

PCC (1997). Criminal Code of June 6, 1997. Journal of Laws of 2022, item 1138, as amended.

PRK (2025). Millions in assets frozen in a case involving a criminal group running fraudulent investment platforms. https://www.gov.pl/web/pr-krakow/29102025-milionowe-zabezpieczenia-w-sprawie-dotyczacej-grupy-przestepczej-prowadzacej-oszukancze-platformy-inwestycyjne [access: 9.08.2026].

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). OJ L, 2024/1689. 12.7.2024.

Regulation 2023/1543 of the European Parliament and of the Council of 12 July 2023 on European Production Orders and European Preservation Orders for electronic evidence in criminal proceedings and for the execution of custodial sentences following criminal proceedings. OJ L 191, 28.7.2023, pp. 118–180.

Report of the Government Plenipotentiary. 2024. Report of the Government Plenipotentiary for Cybersecurity for 2024. https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie, s. 17 [access: 9.08.2026].

Report of the Government Plenipotentiary. 2025. Report of the Government Plenipotentiary for Cybersecurity for 2025. https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie, s. 9 [access: 14.08.2026].

Second Additional Protocol (2022). Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (CETS No. 224).

Ślusarek A., Lange A. (2026). Fake Investment Scams. The Scheme and the Criminal Infrastructure. https://riffsec.com/fake-invest2026/ [access: 9.08.2026].

The Convention on Cybercrime of the Council of Europe (CETS No.185) (2001). https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [access: 9.08.2026].

Tosza S. (2024). Electronic Evidence after E-evidence Package's Adoption: Challenges for Application and Unresolved Problems. Studia Iuridica Lublinensia 33(5), pp. 237–260. https://doi.org/10.17951/sil.2024.33.5.237-260.

U.S. Department of Justice (2025). Chairman of Prince Group Indicted for Operating Cambodian Forced Labor Scam Compounds Engaged in Cryptocurrency Fraud Schemes. https://www.justice.gov/opa/pr/chairman-prince-group-indicted-operating-cambodian-forced-labor-scam-compounds-engaged [access: 1.08.2026].

United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, Resolution 79/243 adopted by the General Assembly on 24 December 2024.

UNTOC (2000). The United Nations Convention against Transnational Organized Crime, adopted by the United Nations General Assembly through resolution 55/25 of 15 November 2000, entered into force on 29 September 2003.