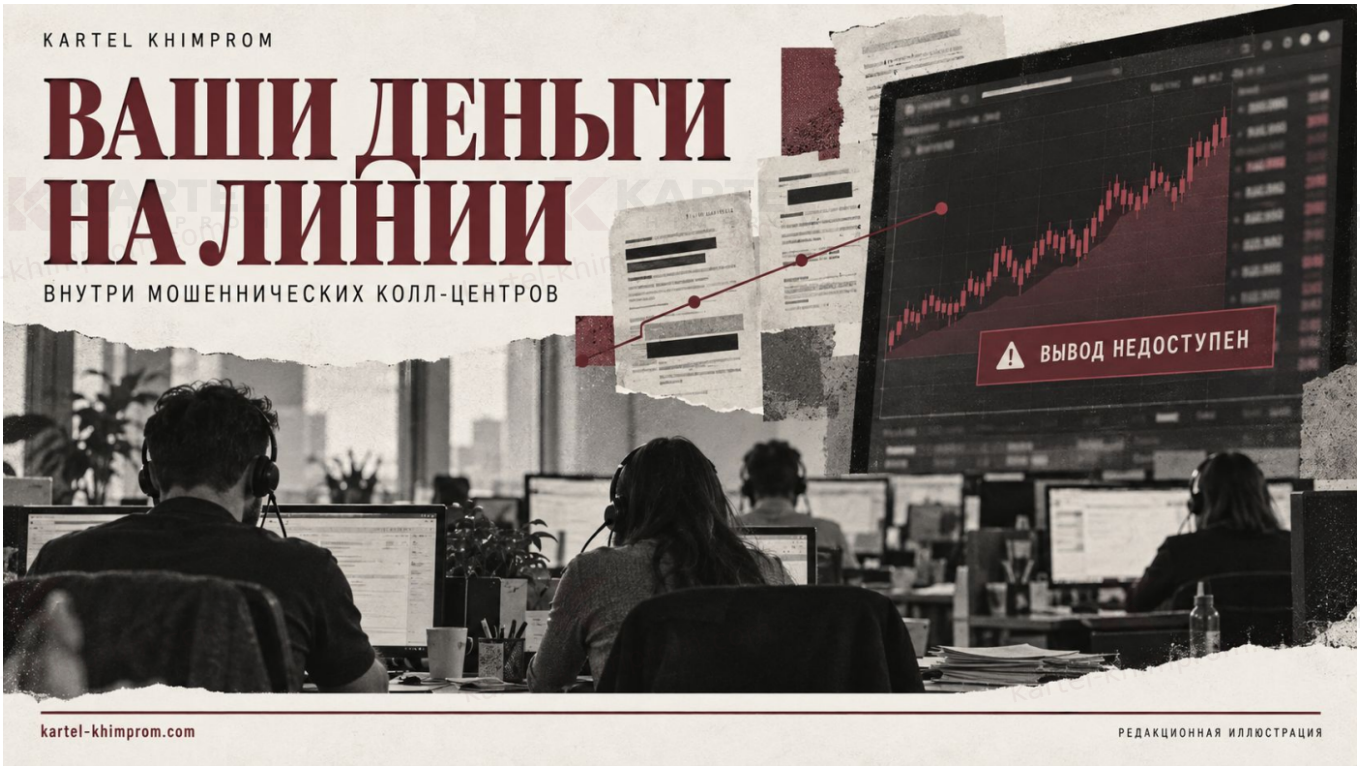
PUBLICATION / EN

Your money is at risk: how the fraudulent call centre industry works

Published 27.09.2026 · Updated 27.09.2026



Your_money_is_at_risk

The money on the screen keeps growing. The money in your bank account is running out. Between these two events lie several weeks of conversations with a man who introduces himself as a financial analyst.

An active link to the original is required when reusing materials

He has a convincing voice, a website full of charts and an answer for every doubt. First, he helps you open an account. Then he suggests increasing your investment. When the customer asks for their money back, a condition is imposed: they must pay more. This is the path – from an advert to a blocked withdrawal – as described by financial regulators and international investigations. Behind it may lie an entire office where other people's savings are turned into a sales scheme.[1][2]

KARTEL KHIMPROM breaks down how this business operates: why fraudsters need their own trading platforms, who works on the phones, how they trick victims into handing over money again, and what is known about the networks operating in Ukraine and beyond.

A stock exchange that customers only see on their screens

Pseudo-Forex uses a familiar financial façade: currency pairs, trades, returns and a personal manager. But the chart alone does not prove that the money has actually been invested. In a case reported by Eurojust in May 2025, the investigation described a completely fraudulent platform: the results shown to clients were used to attract new transfers, whilst the funds received went to the criminal group. At that time, around one hundred victims were known, with total losses exceeding three million euros.[2]

It is incorrect to label the entire foreign exchange market as fraudulent. The CFTC specifically explains that in over-the-counter trading, the client's counterparty may be a dealer. This model in itself does not prove fraud. You need to check the specific company, its licences, terms and conditions, and how it fulfils its obligations. However, a dealer's control over the platform creates opportunities for abuse: the regulator describes cases of price manipulation and the manipulation of trade results, as well as refusals to process withdrawals.[3]

This is precisely where the key question for the 'analyst' arises: apart from the screenshot in your personal account, what evidence is there to confirm your money and your transactions?

Their own platform: a convincing front for other people's money

A fraudulent platform can look quite legitimate: password-protected login, additional verification, a portfolio, transaction history and customer support. The FBI notes that fake investment websites replicate these familiar features and sometimes use names similar to those of genuine financial

services. The presence of a polished interface and even two-factor authentication does not confirm the integrity of its owners.[5]

That said, ‘in-house platform’ does not necessarily mean software written from scratch. The CFTC describes how unscrupulous dealers use popular trading software to make their transactions appear legitimate. The name of a well-known programme is no substitute for checking the organisation that is taking your money.[3]

In this scheme, the screen serves another purpose: it keeps the customer’s attention focused on the profits shown. The client discusses with the manager how much they have supposedly earned, although it would be wise to first find out where the funds they deposited are and who is obliged to return them. This is an editorial conclusion drawn from the cases described by the regulators: a smartly furnished office can distract you from checking the counterparty’s credentials.

Why that first small withdrawal proves nothing

The FCA warns: at the start of the conversation, the customer may indeed receive a small payment. After that, they are persuaded to increase their investment; later, the payments stop, access to the account is restricted, and the firm’s representatives stop responding. Therefore, the argument ‘I’ve already withdrawn money’ does not eliminate the risk of fraud.[4]

These scams often borrow their credibility from someone else’s reputation. According to the FCA, clone firms use the names, registration numbers and addresses of genuinely authorised organisations, whilst substituting the website or contact details. Simply finding a similar name in the register isn’t enough: you need to check whether you’re writing to the right company and have landed on the correct website.[4]

For the reader, this is a practical distinction. It is not a general claim about a ‘licence in Europe’ that is verified, but rather the specific legal entity, its powers and contact details, sourced from an independent official source.

The office operates like a sales department — only it makes money from customers’ losses

In April 2026, Eurojust described an investigation into a network in Tirana: operators were divided into language groups, overseen by team leaders and centre managers. Pay consisted of a basic salary and a commission for successful scams. This organisational structure enabled them to

operate across several national markets simultaneously.[6]

A Ukrainian case, reported by the National Police in December 2025, reveals an even wider range of roles. The investigation listed operators, translators, shift supervisors, IT specialists, technical support staff, security guards, drivers, HR managers, mentors and finance specialists. The call to the victim was merely the visible part of the overall operation.[7]

This leads to a simple conclusion for the investigation: the person wearing the headset is not necessarily the owner. It is necessary to establish separately who hires the staff, pays for the infrastructure, manages the takings and receives the net profit. Arresting an operator and identifying the beneficiary are two different outcomes.

When an ‘analyst’ gains access to your device

Remote assistance can be dangerous if it is imposed by someone to whom you have entrusted your supposed investments. An investigation into a Dnipro-based call centre, published by Eurojust in February 2026, described the use of remote access software to gain control over victims’ funds. The money was transferred to the group’s bank accounts and crypto wallets. The operation resulted in the arrest of eleven people; the investigation is ongoing.[8]

Here, control is lost before the person even realises the money has been debited. They perceive what is happening as routine maintenance of their account. Therefore, a request to enable remote access during a conversation about money should disrupt the usual pattern of trust: first an independent verification, then any actions involving the device.

The latest payment, after which they demand the next one

The culmination of an investment scam is the attempt to take your money. The FBI describes a typical response: the account has been frozen, and an additional ‘tax’ or ‘fee’ is required to unfreeze it. A small withdrawal previously authorised is used as proof that everything is supposedly working. The new payment, however, results in yet another loss.[5]

Then a second round may begin. Another caller introduces themselves as a lawyer, a specialist in recovering funds, or a mediator with government bodies. The FCA calls this a ‘recovery room scam’: the victim is promised that their lost money will be returned in exchange for an upfront fee. The new proposal may be orchestrated by the same fraudsters or by a different team that has obtained

information about the victim.[9]

This is not just a warning from a leaflet. In May 2026, Eurojust reported that a centre in Kharkiv, which targeted elderly people who had already fallen victim to fraud, had ceased operations. According to the investigation, promises to return the money were accompanied by further deception, including fabricated income statements and the drawing up of loan agreements without the victims' knowledge.[10]

Who is behind these networks: names that require evidence

In our editorial archive, we maintain separate sections on 'Khimprom', the Milton Group, 'Devyatki'/'9999', '0900' and other call centre networks. This categorisation helps us to cross-reference reports. It does not imply that the entire market is divided between four owners, nor that all the links attributed to them have already been proven. Non-public editorial information and publicly available documents have different statuses.[15]

'Khimprom'

The link between this name and telephone fraud is mentioned in official documents. In a statement dated 22 April 2026, the National Police of Ukraine linked a network of fraudulent call centres to the activities of 'Khimprom'. The agency identified offices in several regions and put the losses suffered by EU citizens at nearly 50 million hryvnias. This is the investigation's account of the situation; it does not allow us to automatically declare any call centre a subsidiary of the group or to attribute involvement in all incidents to every individual associated with it.[12]

Milton Group and David Todua

A 2020 OCCRP investigation led to the Milton Group's Kyiv office at Mandarin Plaza. Journalists worked with internal documents and interviewed more than 180 victims in various countries. They described the pressure put on clients, fictitious investment returns and the inability to recover their investments.[11]

David Todua is mentioned in the reports. A source identified him as one of the owners; journalists investigated his contacts and links to the payment infrastructure. However, OCCRP separately reported that it had found no evidence of Todua's ownership of the company. Todua himself denied having any formal or informal role in the Milton Group. These caveats form part of the investigation

and cannot be dismissed.[11]

We do not use the term ‘Three Davids’ as a confirmed name for a single management group: the sources verified for this article do not provide sufficient grounds to attribute a specific group of owners to it.

‘9999’ and ‘0900’ numbers

The GI-TOC study ‘Kyiv Calling’, published in April 2026, examines criminal networks in Dnipro and specifically mentions the ‘Nines’, partly on the basis of an interview with a former employee. This confirms the presence of this designation in the research materials, but does not establish the affiliation of every office linked to it online.[13]

‘0900’ is listed separately in our archive: reports received describe it as a different network. In this publication, this distinction remains an editorial classification of the information. The full structure, circle of owners and scale cannot be considered established solely on the basis of recurring nicknames, number plates or the repetition of the same messages.[15]

Protection from the security services: what can be said

The cover-up involving corruption warrants a separate investigation. GI-TOC describes the practice of providing protection to fraudulent call centres and provides evidence of payments for protection and advance warnings of inspections. This information requires a thorough investigation into specific incidents.[13]

However, there is a significant gap in the evidence between ‘an individual employee receiving money for protection’ and ‘the centre belonging to the Main Intelligence Directorate of the Ministry of Defence or the Security Service of Ukraine’. The available evidence does not support the claim that these small offices are established units of these agencies. To reach such a conclusion, documents relating to management, funding and the allocation of revenue are required. A reference to knowing an employee, someone else’s ID card or a story about ‘protection’ is no substitute for this.

Meanwhile, in Eurojust reports on operations in Dnipro and Kharkiv, SBU units are named among those involved in investigations into call centres. This does not rule out the possibility of isolated incidents of corruption, but it illustrates why the role of specific individuals must be assessed separately from the name of the agency.[8][10]

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

The geographical spread of victims is wider than that of the offices

An address in a Ukrainian business centre does not mean that the victims are in Ukraine. In December 2025, Eurojust reported on a network with offices in Dnipro, Ivano-Frankivsk and Kyiv, which was targeting residents of European countries. The investigation identified more than four hundred known victims and estimated the losses at over ten million euros. Staff were recruited from, amongst other places, the very countries whose residents were the targets of the calls.[16]

It is therefore not enough to investigate such schemes within the boundaries of a single city. The telephone operator, the recipient of the transfer, the website owner and the victim may be located in different jurisdictions. Cross-referencing incidents and joint investigation teams in the cases cited are becoming a way of re-establishing the link between these elements.[2][16]

Why does the editorial team need a mailing list?

We have updated our working list of locations based on editorial content from Makondo.net and publicly available documents. It retains sources, disclaimers regarding accuracy, incomplete addresses and possible matches. This is a verification tool, not a list of buildings whose occupants can all be labelled as fraudsters.[15]

For example, a court document relating to a 2023 case in Kyiv contains a list of addresses, details of which were provided to the police. This is historical material; on its own, it does not prove that the same office is still operating at each address today.[17]

For the next step, it is more important to identify a specific tenant and their tenancy period than to add more markers to the map. A mistake in the house number could lead to an innocent company being blamed. A list without dates quickly turns into a list of former addresses.

Addresses mentioned in the editorial material: five cities

Behind these telephone calls lie real premises. Below are specific entries from our editorial archive and a publicly available court document. We have categorised the sources of this information: reports from sources, our own editorial compilation and historical case files.

> **How to read this list.** These are reported locations requiring verification, not a list of confirmed active scam offices. The mention of a building does not imply any involvement on the part of its owner, residents or other tenants. The addresses are not linked to specific criminal groups: separate evidence is required to establish such a connection.

Street names are given as they appear in the source material; some may have been renamed. The date this compilation was updated – 27 September 2026 – does not correspond to the date of observation for each location. Ambiguous numbers, approximate landmarks and private homes are not included in the published section.

Kyiv

- **9 Stepan Bandera Street; Wave-Tower Business Centre** — Historical report from a source regarding a detected office; continued operation has not been confirmed. [21]
- **6 Václav Havel Boulevard** — According to a source; the current operation has not been confirmed. [22][15]
- **74 Antonovych Street; New York Concept House residential complex** — According to a source; the current operation has not been confirmed. [28]
- **49 Vladimirskaya Street** — The source indicates the 4th floor. It is not part of building 49A: the numbering and floor levels differ. [29]
- **56A Yaroslavskaya Street; ‘Canyon’ Business Centre, 4th floor** — Historical note: the source suggests that the office may have already moved. [33]
- **8 Maksimovich Street** — Editorial note; no independent verification available. [15]
- **45/2 Pushkinskaya Street; 5th floor** — Editorial note; no independent verification available. [15]
- **29A Ivan Fedorov Street** — Editorial note; no independent verification available. [15]
- **6 Sosyura Street; ‘Praga’ Business Centre; 5th floor** — Editorial note; no independent verification available. [15]
- **154 Borshchagovska Street** — Editorial note: the same building is mentioned in a court document from 2023. The current operation has not been confirmed. [15][17]
- **22 Verkhniy Val Street** — Editorial note; no independent verification available. [15]

- **31 Pobedy Avenue** — Editorial note; no independent verification available. [15]
- **172 Antonovych Street** — Editorial note; no independent verification available. [15]
- **1B Vadym Hetman Street** — Editorial note; no independent verification available. [15]
- **17A Verbovaya Street** — Editorial note; no independent verification available. [15]
- **55G Bolshaya Vasylkivska Street; 2nd floor** — Editorial note; no independent verification available. [15]
- **101A Vladimirskaya Street; 'Grand Prix' Business Centre** — Editorial note; no independent verification available. [15]
- **49A Vladimirskaya Street; 3rd floor** — Editorial note: no independent verification. Not to be confused with No. 49: the building number and the specified floor differ. [15]
- **35 Mashinostroitelnaya Street; 2nd floor** — Editorial note; no independent verification available. [15]
- **73 Hlubochytska Street; 'Podil Plaza'; 5th floor** — Editorial note; no independent verification available. [15]
- **40 Ushinskogo Street; 3rd floor** — Editorial note; no independent verification available. [15]
- **10A Raisa Okipnaya Street; 22nd floor** — Editorial note; no independent verification available. [15]
- **36-B Yevhen Konovalets Street** — Editorial note; no independent verification. In the previous report, the number suffix was incomplete ('36-'); no match was found. [15]
- **1A Vadym Hetman Street; 1st floor** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **1B Vadym Hetman Street; 3rd floor** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **192 Borshchagivska Street; 'Bizon' Business Centre, floors 5–7** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **2/1 Hrinchenko Street; 'Protasiv Yar' Business Centre** — A court document from 2023; its relevance for 2026 has not been established. Numbers 2/1 and 2 are not combined; they may form part of the same complex. [17]
- **26/8 Metallistov Street; floors 6–7** — Court document from 2023; its relevance for 2026 has not been established. [17]

- **6 Vadym Hetman Street; ‘Cosmopolitan’: Block A, floors 4–6; Block C, floor 6** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **2 Mykola Hrinchenko Street; 5th floor** — A court document from 2023; its relevance for 2026 has not been established. Numbers 2/1 and 2 are not combined; they may form part of the same complex. [17]
- **12 Amosova Street; ‘Horizon Park’, Building 2, 8th floor** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **24 Polevaya Street** — Court document from 2023; its relevance for 2026 has not been established. [17]
- **11 Solomenskaya Street; ‘Eleven’ Business Centre** — Court document from 2023; its relevance for 2026 has not been established. [17]

Dnipro

- **36 Akademika Belelyubskogo Street** — Report from a source; the author is seeking further information. [19]
- **72 Dmitry Yavornytsky Avenue; ‘Delmar Lux’ Business Centre** — According to a source; the current operation has not been confirmed. [20]
- **4 Litaynaya / Livarna Street** — According to a source; the current operation has not been confirmed. [24]
- **16 Filip Orlyk Street; ‘Comfort City’ Business Centre** — According to a source; the current operation has not been confirmed. [25]
- **32 Voskresenskaya Street** — Source confirmation; the archive also contains a rebuttal from the employee in question. Accessing the link to the rebuttal may require access to a restricted channel. [26][27]
- **14 Artelnaya Street** — According to a source; the current operation has not been confirmed. [30]
- **2D Vokzalnaya Square** — According to a source; the current operation has not been confirmed. [31]
- **1 Barrikadnaya Street** — According to a source; the current operation has not been confirmed. [32]

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

Kharkiv

- **43/2 Gagarin Avenue** — Editorial note; no independent verification available. [15]
- **16 Korolenko Street** — Editorial note; no independent verification available. [15]
- **1A Kooperativnaya Street** — Editorial note; no independent verification available. [15]
- **8 Manizera Street** — Editorial note; no independent verification available. [15]
- **9 Prospekt Nauki** — Editorial note; no independent verification available. [15]
- **13 Chernyshevskogo Street** — Editorial note; no independent verification available. [15]

Lviv

- **7 Parkovaya Street** — According to a source; the current operation has not been confirmed. [18]
- **7 Gazovaya Street** — According to a source; the current operation has not been confirmed. [18]
- **321 Gorodotska Street** — Source statement. The sign mentioned in the archive does not establish the involvement of the company of the same name. [23]
- **45 Olena Stepanivna Street** — Editorial note; no independent verification available. [15]
- **2A Pod Goloskom Street** — Editorial note; no independent verification available. [15]
- **7-D Nauchnaya Street; ‘Optima Plaza’ Business Centre; 7th floor** — Editorial note; no independent verification available. [15]

Odessa

- **26 Bolshaya Arnautskaya Street** — Editorial note; no independent verification available. [15]

Links to articles have been saved from the editorial archive; the availability of these posts on Telegram was not re-checked whilst preparing this supplement. A non-public editorial selection is marked with the source [15], which links to the editorial team’s website. The document [17] This information relates to 2023 and is based on reports received by the police; it does not constitute a verdict against all the organisations listed.

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

If you represent an organisation at one of these addresses and have information regarding an error, a change of tenant or the closure of the office, please contact the editorial team. To verify this, we require the date, the specific premises and documents that allow us to check the information. Information about private residents is not required for this purpose.

What to do if you’ve already transferred money

To report the matter to the police, you’ll need proof of payment and a chronology of events. The FBI recommends keeping a record of crypto wallet addresses, amounts, currency, transaction times and transaction hashes, as well as correspondence, the names of websites and apps, the details of the people you’ve been in contact with, and a timeline of your communications. The absence of some information should not prevent you from reporting the matter.[14]

- Keep your receipts and statements, correspondence, the website address and screenshots of your personal account.
- Make a separate note of when and under what pretext you were asked to make each new transfer.
- Don’t assume that paying an unknown ‘refund specialist’ will in itself bring your money back: this could be part of a scam.[9]

The power of this business lies in the gap between the victim’s personal story and the system as a whole. Everyone sees their own ‘analyst’, their own office and their own loss. The job of the investigation is to link these stories to documents, payments and the people who made the decisions.

The editorial team at KARTEL KHIMPROM accepts documented evidence regarding fraudulent platforms and office networks. You can get in touch with us via the contact details on the website or via our official website Makondo.net. When reporting an address, please state the date of observation and the basis for your information. If the information is out of date or contains an error, please send supporting documents for verification and correction.

This article is based on public investigations, reports from law enforcement agencies and the editorial archive. A report of suspicion, the investigation’s version of events and a conviction are not equivalent. The editorial team’s non-public materials are not accessible via the link on its homepage. Date of verification of open sources: 27 September 2026.

Sources

1. FCA — Online trading scams; updated 19 January 2026
   https://www.fca.org.uk/consumers/online-trading-scams
2. Eurojust — International coalition uncovers EUR 3 million online investment fraud; 13 May 2025
   https://www.eurojust.europa.eu/news/international-coalition-uncovers-eur-3-million-online-investment-fraud
3. CFTC — Customer Advisory: What Customers Should Know Before Trading Over-the-Counter Forex; 2 August 2022
   https://www.cftc.gov/PressRoom/PressReleases/8566-22
4. FCA — Forex trading scams; updated 19 January 2026
   https://www.fca.org.uk/consumers/forex-trading-scams
5. FBI / IC3 — Investment Fraud: signs and stages of investment fraud
   https://www.ic3.gov/CrimeInfo/Investment
6. Eurojust — Fraud call centres targeting EU citizens shut down; 29 April 2026
   https://www.eurojust.europa.eu/news/fraud-call-centres-targeting-eu-citizens-shut-down-eurojusts-support-over-eur-50-million
7. National Police of Ukraine — Transnational network of call centres, losses to EU citizens amount to nearly 50 million hryvnias; 16 December 2025
   https://npu.gov.ua/news/natspolitsiia-vykryla-transnatsionalnu-merezhu-shakhraiskykh-call-tsentriv-iaka-oshukala-hromadian-ies-maizhe-na-50-milioniv-hryven
8. Eurojust — 11 arrests during operations against a fraudulent call centre; 23 February 2026
   https://www.eurojust.europa.eu/news/11-arrests-during-actions-against-fraudulent-call-centre
9. FCA — Recovery room scams; updated 19 January 2026
   https://www.fca.org.uk/consumers/recovery-room-scams
10. Eurojust — Scam call centre shut down thanks to a Eurojust-supported investigation; 29 May 2026
    https://www.eurojust.europa.eu/news/scam-call-centre-shut-down-thanks-eurojust-supported-investigation
11. OCCRP — Trail of Broken Lives Leads to Kyiv Call Centre; 2 March 2020, with published clarifications and a response from David Todua
    https://www.occrp.org/en/project/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center
12. National Police of Ukraine — Drug trafficking, violent crime and fraudulent call centres: Khimprom; 22 April 2026
    https://npu.gov.ua/news/narkotorhivlia-nasylnytski-zlochyny-ta-shakhraiski-call-tsentry-natspolitsiia-vykryla-uchasnykiv-zlochynnoi-spilnoty-khimprom
13. GI-TOC — Kyiv Calling: The Scam Call Centre Phenomenon in Ukraine; April 2026, sections on networks and patronage
    https://globalinitiative.net/wp-content/uploads/2026/04/Kyiv-calling-The-scam-call-centre-phenomenon-in-Ukraine-GI-TOC-April-2026.pdf

An active link to the original is required when reusing materials

14. FBI / IC3 — Guidance for Victims of Cryptocurrency Scams; 24 August 2023
https://www.ic3.gov/PSA/2023/PSA230824

15. Makondo.net’s editorial archive — non-public material; link to the editorial website, not to publicly available evidence
https://makondo.net/

16. Eurojust — Fraudulent call centres in Ukraine shut down; 16 December 2025
https://www.eurojust.europa.eu/news/fraudulent-call-centres-ukraine-rolled

17. Solomianskyi District Court of Kyiv — ruling of 20 September 2023, case no. 760/18894/23, document no. 113755670; copy from Opendatabot
https://opendatabot.ua/court/113755670-447f218b240291db6fbe07c7b7614ae6

18. Editorial archive: report from source No. 35; location details, relevance not confirmed
https://t.me/budda_sop/35

19. Editorial archive: report from source No. 348; location details, accuracy not verified
https://t.me/budda_sop/348

20. Editorial archive: report from source No. 477; location details provided, validity not confirmed
https://t.me/budda_sop/477

21. Editorial archive: source report No. 637; location details, validity not confirmed
https://t.me/budda_sop/637

22. Editorial archive: report from source No. 1215; location details, accuracy unconfirmed
https://t.me/budda_sop/1215

23. Editorial archive: report from source No. 1241; location details, validity not confirmed
https://t.me/budda_sop/1241

24. Editorial archive: report from source No. 1385; location details; accuracy not confirmed
https://t.me/budda_sop/1385

25. Editorial archive: source report No. 1432; location details, validity not confirmed
https://t.me/budda_sop/1432

26. Editorial archive: source report No. 1463; location details, validity not confirmed
https://t.me/budda_sop/1463

27. Editorial archive: report from source No. 594 containing the aforementioned employee’s rebuttal; private channel
https://t.me/c/3846282687/594

28. Editorial archive: source report No. 1494; location details; validity not confirmed
https://t.me/budda_sop/1494

An active link to the original is required when reusing materials

29. Editorial archive: report from source No. 1501; location details and accuracy not confirmed
https://t.me/budda_sop/1501

30. Editorial archive: report from source No. 1560; location details and accuracy not confirmed
https://t.me/budda_sop/1560

31. Editorial archive: source report No. 1583; location details, validity not confirmed
https://t.me/budda_sop/1583

32. Editorial archive: tip-off No. 1838; location details, accuracy not confirmed
https://t.me/budda_sop/1838

33. Editorial archive: tip-off No. 2227; location details; accuracy not confirmed
https://t.me/budda_sop/2227

Use of materials

An active link to the original publication is required when using these materials.

Original publication

https://kartel-khimprom.com/en/article/your-money-is-at-risk-how-the-fraudulent-call-centre-industry-works/