PUBLICATION / EN

Dnipro’s Myanmar: call centres, “Nines” and money behind the office façades

Published 15.10.2026 · Updated 15.10.2026



Five raids, 178 pieces of computer equipment, six Starlink terminals and two hardware crypto wallets. This is what one episode in the crackdown on fraudulent call centres in Dnipro in 2026 looks like. Behind this inventory lies a question that the photograph of the seized computers does not answer: who managed the operation, who facilitated the flow of money, and who reaped the lion’s share of the profits? [4]

An active link to the original is required when reusing materials

It is easy to tell the story of Dnipro's 'offices' through the lens of yet another arrest. It is far more difficult to trace how individual teams are linked to the organisers and financial intermediaries. In this article, we compare official reports on the investigations, an international study and a dossier from our from the '9999' archive — 'Nines'.

These sources have different statuses. Police reports convey the investigation's version of events in specific cases; the research report describes the market; personal dossiers contain attributed information from the editorial team's sources. In the reports on the 2026 operations discussed below, the police do not name the six individuals whose profiles are included in the article, nor do they establish their involvement in these incidents.

Dnipro: a scale that cannot be gauged by a single raid

In the April GI-TOC report *Kyiv calling: The phenomenon of scam call centres in Ukraine* Dnipro and Kyiv are cited as major hubs for this industry. The authors cite an estimate of approximately 30,000 workers in Dnipro's 'offices' by the end of 2024. This is an estimate reproduced by the researchers, not a census of the workforce, nor a figure for October 2026. [1]

The report makes specific mention of the 'Nines': a former employee describes threats and severe restrictions when moving to competitors. This section is based on an interview rather than a judicial determination of each episode described. The authors themselves emphasise the difficulties of verifying a closed environment. [1]

For the reader, the scale of the task is important here. Even a compelling report on a single office does not provide a complete picture of the city. Nor does a high estimate of the number of workers automatically mean that all employees can be attributed to a single group. Answering the question about the network requires establishing links between specific sites, people and payments.

Four reports from 2026: what exactly did the law enforcement agencies uncover?

Below are specific operations and activities. The dates in the table refer to official publications; they do not always coincide with the dates of the searches.

Date of post	Geography and the investigation's version of events	Published result
1 April 2026	Dnipro. Dating and the pretence of personal relationships were used to lure people into bogus crypto investments.	Eight people have been detained; according to the National Police of Ukraine, over $2 million has passed through the accounts. [2]
21 May 2026	Dnipropetrovsk Oblast. Fraudulent calls from banks and transfers to supposedly secure accounts.	22 identified victims, nearly 3 million hryvnias in losses, 40 searches, ten suspects. [3]
12 August 2026	Kamenskoye, Dnipropetrovsk Oblast. A call centre which investigators link to embezzlement from Israeli citizens.	At least five victims; reported losses of nearly 1.7 million hryvnias; nine detainees have been served with notices of suspicion. [5]
1 September 2026	Dnipro. Posing as bank and mobile operator staff to gain access to bank accounts.	Following searches carried out on 27 August, equipment, communication devices, crypto wallets and over 600,000 UAH in cash were seized. [4]

These figures cannot be added together to give the total 'turnover of the Dnipro mafia'. Funds passing through accounts, established losses and cash found are different indicators. The seizure of assets also does not mean that their criminal origin has already been proven.

The April Case: an introduction as a gateway to a financial trap

In a statement dated 1 April, the National Police of Ukraine (NPU) described its work with victims from Ukraine and other countries, including Kazakhstan and Lithuania. According to the investigation, contact began on dating sites and via messaging apps, after which the victim was

persuaded to invest in cryptocurrency. Fake accounts were used, and the perpetrators disguised their identities during video calls. [2]

The police reported on the division of roles: coordinators, department heads, victim support teams and a technical unit. After the victim's initial investment, 'analysts' would be assigned to them; under the guise of offering assistance, these individuals gained access to confidential data and assets. During the searches, ten luxury cars and over $100,000 in cash, amongst other items, were seized. The agency reported suspicions of forming and participating in a criminal organisation and of particularly large-scale theft. [2]

A distinctive feature of this type of scam is the gradual change in the relationship. The victim may believe they are trusting someone they know, even though they are actually being dealt with by a succession of different operatives. To investigate such a case, the history of correspondence and the handover of contact details between staff members are crucial: they can reveal whether there was an overarching plan behind what appeared to be a personal conversation.

A banking legend: fear instead of the promise of profit

A May report by the National Police of Ukraine describes another method of operation. People were warned about fictitious suspicious transactions, loans or card blocks, and persuaded to transfer money to 'safe' accounts. Investigators traced the scheme's operations to the period from September 2025 to May 2026; the money flows involved accounts held by front men and cryptocurrency exchanges. At the time of publication, eight suspects had been remanded in custody, subject to bail. [3]

The Cyber Police's September report also mentions accounts held by front men. According to the investigation, the funds were then withdrawn via ATMs in Dnipro or converted into virtual assets. The number of victims and the final amount of the losses were still being determined at the time of the report. [4]

The Kamensk incident highlights the international dimension of the problem: according to the regional police, the perpetrators posed as employees of banks, telecoms operators or internet service providers and gained access to the online banking accounts of Israeli citizens. Kamensk is a separate town; it would be a mistake to place this office on a map of Dnipro itself. [5]

‘Nines’: who is mentioned in our archive and on what grounds

In in the ‘9999’ section Personal profiles have been compiled based on publications and source materials. These are useful for cross-referencing names and presumed roles. However, several profiles based on a single report do not constitute multiple independent confirmations. The following disclaimers regarding the origin of the information and the limits of its verification are provided below.

Igor Khromov: the presumed leadership circle

In A profile of Igor Igorevich Khromov The file contains reports from a source who places him within the leadership circle of ‘9999’ and links him to the organisation of call centres. The profile also examines references to sports organisations. This is information from the source: specific powers and involvement in individual operations require separate verification. [6]

> **Igor Igorevich Kromov**
>
> The source identifies Igor Khromov, known as ‘Zhaba’, as a member of the leadership circle of the ‘9999’ organisation.

Konstantin Gavrilenko: the theory about managing the network

A profile of Konstantin Nikolayevich Gavrilenko reports a source's claim regarding a leadership role in '9999' and control over the network of offices. The report cites material from the editorial team's internal database as its basis; there is no public link to the original record. Therefore, the version presented here is not equivalent to a published court ruling regarding ownership of specific call centres. [7]

> **Konstantin Nikolaevich Gavrilenko**
>
> According to a source, Konstantin Gavrilenko, known as 'Nikolaich', is a member of the leadership of the '9999' organisation and controls a network of call centres.

Vyacheslav Kapustin: the question of how the money is distributed

In A report by Vyacheslav Kapustin The source attributes to him the distribution of funds amongst the managers of '9999'. The report draws on internal documents and explicitly states that the list of companies does not establish the source of their income. [8]

> **Vyacheslav Kapustin**
>
> The source names Vyacheslav Kapustin as the person responsible for distributing funds amongst the leaders of the '9999' organisation.

To verify this theory, documents relating to the handling of funds would be crucial: payments, signatory authorisations, accounting records and the link between transactions and specific victims. The mere existence of a business or an acquaintance with another person implicated in the case does not replace this chain of evidence. We examined the business context separately in the article 'Vyacheslav Kapustin and Alexander Petrovsky: new companies, old connections'.

An active link to the original is required when reusing materials

Yevgeny Chepurnov: sports projects and statements from a source

In A profile of Yevgeny Sergeyevich Chepurnov The source links him to Khromov and projects known as ‘Vataga’. The same source also alleges the use of sporting activities to launder proceeds — with the explicit caveat that this has not been independently confirmed. We maintain this distinction: membership of a sporting organisation does not in itself prove a financial offence. [9]

> **Yevgeny Sergeyevich Chepurnov**
>
> The source identifies Yevgeny Chepurnov as a member of ‘9999’ and a partner of Igor Khromov.

Sergei Mereško: a historical reference to the administrator

Sergei Nikolaevich Mereško The source names the office administrator as being linked to Gavrilenko. The profile itself states that the current composition of the administration requires clarification. Consequently, this refers to the period described by the source, rather than a position confirmed as of today. [10]

> **Sergey Nikolaevich Mereško**
>
> The source describes Sergei Mereško as an office administrator who is linked to Konstantin Gavrilenko and the ‘9999’ network in Dnipro.

Yevhen Chumachok: why the accuracy of a role is important

An active link to the original is required when reusing materials

A profile of Yevgeny Ruslanovich Chumachok contains a correction to the original description: the source refers to him as a senior closer, not an administrator, and attributes the leadership of a separate team within the Gavrilenko network to him. This information remains the source's assertion. [11]

> **Yevgeny Ruslanovich Chumachok**
>
> According to a source, Yevgeny Chumachok heads his own team within Konstantin Gavrilenko's office network.

The difference between roles is significant. Leading a customer service team, managing the premises and disposing of the overall takings entail different levels of authority. It is easier to lump everyone together under the term 'organisers' than to establish exactly what decisions each person made. Yet it is precisely the individual role that determines what can reasonably be written about a person.

Where does 'Khimprom' fit into this story?

GI-TOC regards the Dnipro networks and 'Khimprom' as distinct major components of the market. Researchers suggest that 'Khimprom's' shift towards fraud may have utilised infrastructure and personnel previously involved in drug trafficking. The report provides no grounds for considering the 'Nines' to be a division of Burkin's organisation or for grouping all the Dnipro offices under a single leadership. [1]

A separate story is that of the case of the Moscow call centres and their alleged links to 'Khimprom'. It makes sense to compare such cases based on the people involved, the payments and the infrastructure. A shared investment narrative or the use of cryptocurrency does not necessarily imply a common owner.



What should remain after a search, apart from photographs of the equipment?

A criminal case becomes clearer when a chain of evidence emerges alongside the number of computers. To assess the outcome of the investigation, we suggest considering five questions:

1. **Who made the decisions?** Have the people who appointed managers, authorised expenditure and determined the allocation of work been identified?

2. **Who was making the money?** Has the flow of funds been traced beyond the recipient’s first account, and have any assets been found that can be linked to the embezzlement?

3. **How are the offices connected?** Is there any evidence of centralised management, or are we dealing with different groups using similar methods?

An active link to the original is required when reusing materials

4. **What confirms each individual’s role?** Are there any documents, correspondence, witness statements and technical data that are consistent with one another?
5. **What happened next with the case?** Have charges been brought, has a trial taken place, how has the evidence been assessed, and has the issue of compensation been resolved?

Allegations of patronage deserve special attention. Concrete actions are also required here: warning of a search, passing on official information, receiving remuneration or interfering with proceedings. The mere fact that an office has been operating for a long time does not prove the guilt of a particular official. However, confirmed interference can explain why the activities continued.

Behind the term ‘office’ lies a victim

In the news feed, it’s easier to remember cars, sums of money and nicknames. For someone who has lost their savings, the main outcome is different: the recipients of the money have been identified, evidence has been preserved, and a decision on compensation has been reached. That is precisely why the investigation into the Dnipro call centres is worth reading beyond the headline about the arrests.

Our archive allows us to track personal mentions and trace them back to their sources. Official records provide verifiable details. The next task is to establish where these lines actually intersect. Where a connection is confirmed, it must be highlighted; where there is only speculation, the investigation must continue.

Follow this topic: reports and articles on the ‘Nines’. Previous articles on this topic: Dnipro call centres, ‘drops’, cash and cryptocurrency.

Sources

1. GI-TOC — Kyiv calling: The scam call centre phenomenon in Ukraine, April 2026; pages 7 and 14

An active link to the original is required when reusing materials

https://globalinitiative.net/wp-content/uploads/2026/04/Kyiv-calling-The-scam-call-centre-phenomenon-in-Ukraine-GI-TOC-April-2026.pdf

2. Ukrainian National Police — a network of call centres in Dnipro and the theft of crypto-assets, 1 April 2026
   https://npu.gov.ua/news/politseiski-likviduvaly-u-dnipri-merezhu-kol-tsentriv-cherez-iaki-vykradaly-kryptoaktyvy-zatrymano-8-orhanizatoriv
3. Ukrainian National Police — pseudo-bankers and nearly 3 million UAH in losses, 21 May 2026
   https://npu.gov.ua/news/politsiia-dnipropetrovshchyny-zatrymala-psevdobankiriv-iaki-oshukaly-hromadian-na-maizhe-3-mln-hrn
4. Ukraine’s Cyber Police — a call centre in Dnipro, searches on 27 August and 178 pieces of equipment, 1 September 2026
   https://cyberpolice.gov.ua/news/u-dnipri-policziya-prypynyla-diyalnist-shaxrajskogo-call-czentru-vylucheno-majzhe--odynycz-kompyuternoyi-texniky-4651/
5. Dnipropetrovsk Regional Police — a call centre in Kamensk and victims from Israel, 12 August 2026
   https://dp.npu.gov.ua/news/na-dnipropetrovshchyni-politsiia-vykryla-uchasnykiv-zlochynnoi-orhanizatsii-iaki-oshukala-hromadian-izrailiu-na-maizhe-17-miliona-hryven
6. KARTEL KHIMPROM — Igor Igorevich Khromov, file no. 1353
   https://kartel-khimprom.com/ru/dossier/hromov-igor-igorevich/
7. KARTEL KHIMPROM — Konstantin Nikolaevich Gavrilenko, file No. 0758
   https://kartel-khimprom.com/ru/dossier/gavrilenko-konstantin-nikolaevich/
8. KARTEL KHIMPROM — Vyacheslav Kapustin, file No. 0920
   https://kartel-khimprom.com/ru/dossier/kapustin-vyacheslav-2/
9. KARTEL KHIMPROM — Yevgeny Sergeyevich Chepurnov, file No. 1362
   https://kartel-khimprom.com/ru/dossier/chepurnov-evgenij-sergeevich/
10. KARTEL KHIMPROM — Sergei Nikolaevich Mereshko, file No. 1074
    https://kartel-khimprom.com/ru/dossier/mereshko-sergej-nikolaevich/
11. KARTEL KHIMPROM — Yevgeny Ruslanovich Chumachok, file no. 1380
    https://kartel-khimprom.com/ru/dossier/chumachok-evgenij-ruslanovich/

Use of materials

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

Original publication

https://kartel-khimprom.com/en/article/dnipros-myanmar-call-centres-nines-and-money-behind-the-office-fa%c3%a7ades/