PUBLICATION / EN

Call-centre network dismantled in Dnipro: money was channelled via ‘drop accounts’, cash and cryptocurrency

Published 02.10.2026 · Updated 02.10.2026

The National Police of Ukraine have announced that they have dismantled a network of fraudulent call centres in Dnipro. According to the investigation, the group operated by sending messages about fictitious lottery wins, using ‘drop’ bank cards, making cash withdrawals and converting funds to cryptocurrency via P2P transactions. The court has not yet established the guilt of those involved.

An active link to the original is required when reusing materials



In Dnipro, the police announced that they had shut down a network of fraudulent call centres through which, according to the investigation, money stolen from members of the public was channelled via ‘drop’ bank cards, withdrawn as cash and converted into cryptocurrency. An official statement from the Department of Strategic Investigations of the Ukrainian National Police was published on 1 October 2026 at 14:00; its contents were also reported by UNN and Ukrinform. Direct access to the National Police of Ukraine’s webpage via the editorial tool was partially blocked, but the indexed text of the official press release is available in search results at npu.gov.ua.

According to the investigation, a network of fraudulent call centres was operating in Dnipro, organised by a group of individuals with clearly defined roles. For this operation, as reported by the National Police, the suspects rented two premises in the city: some members supervised the operators and the flow of money, whilst others were responsible for issuing bank cards in the names of front men, cashing out funds and converting them into cryptocurrency.

The scheme: a ‘win’ notified via a messaging app and a card in someone else’s name

The key entry point to the scheme, according to the investigation, was simple: messages about alleged winnings were sent en masse to members of the public via Telegram and Viber. Afterwards, the victims’ money, the police claim, ended up in accounts registered in the names of third parties.

An active link to the original is required when reusing materials

UNN, citing the National Police's Press Service, reports that the messages concerned fictitious winnings, and the funds obtained fraudulently were withdrawn via 'drop' cards and converted into cryptocurrency.

A separate component of the scheme involves 'drops'. Ukrinform, citing the National Police of Ukraine's Department of Special Investigations, explains that in the press release this term refers to people who, in return for payment, provide fraudsters with access to their bank cards and accounts. According to the investigation, the suspects posted advertisements on social media offering to purchase personal and identification data required to open bank accounts and set up online banking services.

The National Police claim that the scheme involved not only 'professional drop accounts' but also students, pensioners and the unemployed. According to the investigation, accounts and payment cards were opened in their names, whilst the group's members retained actual control over them. The victims' money was then transferred into these accounts; the funds were subsequently withdrawn via ATMs or converted into cryptocurrency using P2P transactions.

What was found during the searches

As part of the criminal proceedings, law enforcement officers carried out 21 searches in Dnipro and the Dnipropetrovsk region. According to the National Police of Ukraine, investigative operations took place at the call centres' premises, at the suspects' homes and in their vehicles; Operatives from the Strategic Investigations Department in the Dnipropetrovsk region, regional police investigators, special-purpose police units and KORD were involved.

The list of seized items highlights the infrastructural nature of the case. The official statement lists over 40,000 euros, 18,000 dollars and 113,000 hryvnias, as well as weapons and ammunition, 158 mobile phones, 35 items of computer equipment, 13 storage devices, 25 SIM cards, 153 SIM card holders, 10 bank cards and two Starlink kits. Furthermore, according to police reports, documents, draft notes and nine cars were seized, including an Audi S8, RS7 and A6, a Land Rover Range Rover Evoque, a BMW X6M and 535XI, a Toyota Land Cruiser 200, a Subaru Forester and a Cupra Formentor.

Investigators also claim that the suspects used part of the criminally obtained funds to purchase property, premium-class cars, expensive watches, jewellery and other highly liquid assets. This information remains, for the time being, merely the investigation's version of events: the materials

An active link to the original is required when reusing materials

examined do not contain any public court rulings that would confirm the origin of the assets or the guilt of specific individuals.

Procedural status

According to the National Police, the pre-trial investigation is continuing as part of criminal proceedings on charges of fraud, under the procedural supervision of the Dnipropetrovsk Regional Prosecutor’s Office. The official press release and reports by UNN, Ukrinform and local media do not specify the names of those involved, nor do they provide details regarding the service of charges, arrests, the preventive measures imposed, the number of victims or the total amount of losses.

Important: All accusatory statements in this article refer to the investigators’ version of events. The court has not established the guilt of the individuals involved. The National Police also draws attention to Article 62 of the Constitution of Ukraine: a person is presumed innocent until their guilt has been proven in accordance with the law and established by a court conviction.

At the time of writing, no public comments had been found from the suspects, their lawyers or representatives of the premises they had rented. Therefore, this case should correctly be regarded not as a concluded legal proceeding, but as a recent example of the kind of infrastructure which, according to law enforcement, fraudulent call centres may use: messaging apps for initial contact, ‘drop boxes’ for bank transfers, and cash and P2P crypto transactions for the subsequent withdrawal of funds.

Sources

1. Fictitious winnings and a network of ‘drop accounts’ for withdrawing funds: police in Dnipro have shut down fraudulent call centres — National Police of Ukraine
   https://npu.gov.ua/news/fiktyvni-vyhrashi-ta-merezha-dropiv-dlia-vyvedennia-koshtiv-u-dnipri-politsiia-prypynyla-diialnist-shakhraiskykh-call-tsentriv

2. Fraudulent call centre network exposed in Dnipro — Ukrinform
   https://www.ukrinform.ua/rubric-regions/4170218-u-dnipri-vikrili-merezu-sahrajskih-kolcentriv.html

3. Fake winnings and a network of ‘drop accounts’ for withdrawing funds: police in Dnipro have shut down fraudulent call centres — Dnipro City Website
   https://m.gorod.dp.ua/news/264137

4. Large-scale network of fraudulent call centres dismantled in Dnipro — MIC
   https://mis.dp.ua/ru/novosti/v-dnepre-likvidirovali-masshtabnuyu-set-moshennicheskih-kol-czentrov

An active link to the original is required when reusing materials

Use of materials

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

Original publication

https://kartel-khimprom.com/en/article/call-centre-network-dismantled-in-dnipro-money-was-channelled-via-drop-accounts-cash-and-cryptocurrency/