

INVESTIGATIONS / SOURCE EDITION / EN

FRAUD EMPIRE

Telephone scams, psychological manipulation and illicit money flows. An in-depth report examining call-centre networks, their victims, and the connections and investigations described in the original article.

TRUTH magazine | 09.09.2026



TRUTH Magazine · AI-generated editorial illustration

Reprint of an article published on LinkedIn.



Zeljka Zorz, Editor-in-Chief, Help Net Security December 16, 2025

How Ukrainian call centers became Europe's largest Financial Mafia

A source-checking update dated 30 October 2026 appears at the end of this article, with important distinctions about amounts, investigations and uncorroborated claims.

When #Volodymyr #Zelenskyy was asked about illegal call centers by an investigative journalist from #UkrainskaPravda during a 2023 press conference, the President brushed it off with a vague assurance that law enforcement was working on the issue. At the time, no one suspected that this enigmatic phrase concealed an organized crime syndicate generating revenues of up to a billion dollars a month. For years, it robbed citizens across Europe with impunity, its tentacles reaching the highest levels of the prosecutor's office, the Security Service of Ukraine (SSU), and parliament.

Today, following NABU and SAPO's joint operation codenamed "Carthage," we know this was merely the tip of the iceberg. In just a few days, authorities exposed a mechanism that enabled a billion-dollar-a-month fraud empire to operate right at the very heart of the justice system.

I. A Phenomenon on a Continental Scale The City That Became the Capital of Fraud

Fraudulent call centers operating from Ukraine have robbed citizens of at least 29 countries—from Germany, Poland, and the Czech Republic, to the United States, Canada, and even Australia. According to data from German authorities, Ukrainian perpetrators were responsible for 40% of all fraudulent phone calls registered in Germany in 2025.

The profile of the victims is particularly striking: a staggering 85% are citizens of Ukraine and European nations. Russian citizens account for merely 10–15%. Therefore, the scheme primarily targets Ukrainians themselves and their European neighbors, rather than—as one might assume—Russian citizens.

The scale of employment within these criminal structures reaches 60,000 people. This is not just a statistic; it is a daily reality in which young Ukrainians, instead of building a legitimate economy, choose quick and easy money. As investigative journalist Mykhailo Tkach ironically noted: "I think we will know we've achieved a result when 500,000 twenty-somethings driving BMWs and carrying Louis Vuitton bags suddenly start looking into how to install LPG tanks in their cars."

At its peak, the network controlled approximately 500 call centers across the country. With a extortion fee of \$7,000 per center monthly, it generated \$3.5 million in illegal revenue—flowing directly into the pockets of corrupt officials.

II. The Anatomy of Fraud – How It Works From Cold Call to Empty Account

The process of defrauding a victim is a strictly hierarchical procedure, with each stage executed by distinct specialists:

- Administrators – Oversee office operations and manage employee training.
- HR Managers – Handle recruitment, payroll, and financial tracking.
- "Cold Callers" – First-line operators responsible for making initial contact with potential targets.
- "Closers" – Highly experienced fraudsters who take over the line whenever a victim shows doubt, ultimately pressuring them into transferring funds.
- IT Specialists – Manage the technical infrastructure, deploy fraudulent investment platforms, and maintain malicious software.
- Mentors & Trainers – Onboard and instruct new hires on psychological manipulation.

The scheme begins with a cold call. The operator contacts the target, impersonating a bank representative, law enforcement officer, judge, or intelligence official. The victim is informed, for

instance, that they are under criminal investigation or that unauthorized perpetrators are attempting to breach their bank account.

If the target displays interest or distress, the communication is immediately shifted to encrypted messaging apps (WhatsApp, Telegram), where the "closers" step in. Employing threats, blackmail, and intense psychological leverage, they coerce the victim into making wire transfers. If they determine the victim is sufficiently terrified, they push them to liquidate assets, sell real estate, or take out high-interest bank loans.

Psychological Tools of Manipulation

Operators undergo training in basic behavioral psychology. They learn not only to read pre-written scripts but also to emotionally hook the target. Key techniques include:

- **Establishing Authority:** Impersonating law enforcement officers or government officials. Utilizing leaked databases, they recite authentic personal details—card numbers, passwords, and family information—to build credibility.
- **Inducing Fear:** Threatening targets with fictitious criminal charges, imminent arrest, or total asset forfeiture. Fear paralyzes rational decision-making.
- **Isolating the Target:** Instructing victims to maintain absolute secrecy "for the integrity of the investigation," severing them from family support or professional advice.
- **Creating False Security:** Presenting a "safe" solution: transferring funds to a "protected account" or installing a "security application" that is, in reality, a trap.
- **Time Pressure:** Demanding immediate action to prevent any opportunity for outside consultation or verification.

The Role of Emerging Technologies

Artificial intelligence has become a core operational multiplier in this industry:

- **Voice Cloning:** AI models replicate the exact voices of acquaintances or relatives, instantly dismantling the victim's skepticism.
- **Deepfakes:** Perpetrators generate AI video profiles of alleged officials and send them to targets to intensify psychological pressure. In May 2026, police in Odesa dismantled an international syndicate that used deepfakes to defraud citizens across Kazakhstan.
- **Automated Translation:** Real-time AI translation tools allow operators to execute schemes in foreign languages fluently, enabling simultaneous attacks across dozens of jurisdictions.
- **Fraudulent Investment Platforms:** Websites engineered to mirror major cryptocurrency exchanges. Targets believe they are trading assets, unaware they are granting fraudsters direct access to their wallets.

- Remote Access Malware: Victims are lured into downloading fake banking applications that grant criminals total remote control over mobile devices and bank accounts.
- Automated Document Forgery: Proprietary software generates falsified institutional correspondence featuring authentic target data within seconds.

Primary Fraud Schemes

- The "Bank Official" Scam: The most widespread method across Europe. Fraudsters report a breach and urge immediate transfers to "safe accounts."
- The "Police Officer" Scam: Prevalent in Poland and the Czech Republic. Operators pose as law enforcement agents and threaten targets with arrest.
- Crypto Investment Fraud: Victims are drawn to fraudulent trading engines. Initial "investments" yield artificial profits to build trust before large sums are deposited and erased.
- Romance Scams: Cultivating long-term online relationships to build emotional reliance before manufacturing financial emergencies.
- The "Tax Authority" Scheme: Primarily targeted at victims in Germany and the United States using threats of fake tax liabilities.

Facility Security – How Operations Avoid Detection

Paradoxically, these illicit call centers operate in plain sight, leasing prime office spaces in central commercial districts. However, their physical and operational security measures are rigorous:

- Surveillance cameras monitoring every angle and workstation.
- Electronic access control systems and physical security details.
- Polygraph examinations used during onboarding to identify undercover officers, journalists, or informants.
- Mandatory confiscation of personal mobile devices upon entry.
- Continuous monitoring of computer activity and screen keystrokes.
- Complex 20–30 character passphrases and full-disk encryption.
- Restricted software access bound exclusively to dedicated IP ranges.
- Anonymous operational accounts, foreign SIM cards, and private Telegram channels.

New recruits are openly scouted via TikTok, Telegram, and public job boards under the guise of "customer relationship manager" positions—or even as baristas and barbers—before being systematically absorbed into criminal operations.

III. Operation "Carthage" – how NABU dismantled the prosecutorial Syndicate The Night That Shook Kyiv

Late on the evening of September 4, 2026, operatives from the National Anti-Corruption Bureau of Ukraine (NABU) and the Specialized Anti-Corruption Prosecutor's Office (SAPO) raided the Office of the Prosecutor General in Kyiv. Law enforcement executed search warrants across the offices and private residences of Prosecutor General Ruslan Kravchenko, his First Deputy Maria Wdowychenko, and several senior prosecutors.

Codename Operation "Carthage," the sweep represents one of the largest anti-corruption crackdowns in independent Ukraine's history. NABU officially announced the dismantling of a organized criminal enterprise operating within the Prosecutor General's Office, whose members systematically extracted kickbacks from fraudulent call centers in exchange for high-level protection and total immunity.

The Central Figure – Serhiy Kropyva, Alias "The Chancellor"

At the center of the conspiracy stands 42-year-old Serhiy Kropyva, Deputy Head of the Department for International Legal Cooperation at the Prosecutor General's Office. Prior to his prosecutorial appointment, Kropyva served as Deputy Head of the Odesa Regional Military Administration for Digital Development, and until 2022, held the post of First Deputy Head of the Cyber Police Department of the National Police of Ukraine. In short: the official tasked with eradicating cybercrime had become its primary patron.

According to investigators, Kropyva orchestrated the security apparatus shielding these call centers. His role was to ensure no criminal proceedings threatened fraudulent operations, collecting recurring extortion fees in return. Investigators estimate Kropyva amassed assets exceeding 89 million UAH (approximately \$2 million).

On September 6, the High Anti-Corruption Court remanded Kropyva into custody until November 2, setting bail at 120 million UAH (approx. \$2.7 million). Defense counsel announced plans to appeal.

Wiretaps and Incriminating Audio

NABU released intercepted audio recordings exposing not only the scale of the corruption, but the brazen arrogance of the prime suspects. In one wiretapped exchange, Kropyva states:

"I can't just go to work for the sake of working. Living just to live. If I do something, it has to be huge. I prefer to live like royalty. Fuck it—screw the queen, steal a million."

The recordings also revealed Kropyva managed the ongoing renovation of Prosecutor General Kravchenko's private residence in Kozhyn—overseeing the installation of gas generators, power inverters, backup battery systems, and security alarms—and even coordinated repairs on an

icebreaker vessel. Furthermore, Kropyva procured flight tickets to Spain for Kravchenko and his wife, which were fraudulently logged in official documentation as state business trips.

During the bail hearing, SAPO Prosecutor Mykola Karas read aloud excerpts from conversations between Kropyva and Kravchenko: "Yes, Andriyovych. Yes, Boss. No, everything is fine. No, nobody is bothering me. Who would bother me? You're covering for me. That's why everybody knows."

The Inner Circle – "The Muse," "Comrade," and Co-Conspirators

The investigation named five primary targets under Article 255 (Creation and Leadership of a Criminal Organization) and Article 209 (Money Laundering) of the Criminal Code of Ukraine, carrying sentences of up to 15 years in prison.

- Yelizaveta Ivakhnenko (24): Kropyva's partner, referred to in investigative files as "The Muse" or "The Queen." The court ordered her detained for 60 days with bail set at 20 million UAH (approx. \$460,000). Investigators state Ivakhnenko served as the primary conduit for laundering call-center revenues, placing funds into accounts held by her and her immediate family. She was reportedly slated for an upcoming appointment as Deputy Minister of Education.
- Serhiy Kut: Kropyva's personal driver, identified as "Comrade" in the wiretaps, remanded with bail set at 3 million UAH.
- Oleksandr Dydych: An attorney and Kropyva's brother-in-law, detained with bail set at 15 million UAH. Dydych assisted in concealing assets by shuffling real estate holdings across network entities.



Safes Loaded with Cash and Luxury Real Estate

Following the raids, NABU published images of an open safe overflowing with stacks of cash in USD and EUR. Although Prosecutor General Kravchenko denied ownership of the safe or its presence in his office, the imagery became the defining emblem of the scandal.

Investigative journalists from Hromadske established that Kropyva's family and associates acquired assets exceeding \$1 million in recent years. Official records show Kropyva himself acquired no properties throughout his tenure in public service, save for a privatized apartment in Zolotonosha. Meanwhile, his 64-year-old mother regularly posted social media updates from luxury vacations in Cyprus and Hawaii. The rapid accumulation of family assets coincided directly with Kropyva's 2020 appointment as First Deputy Head of Cyber Police.

Resignation of the Prosecutor General

While Kropyva remains the primary suspect, severe suspicion immediately fell upon Prosecutor General Ruslan Kravchenko. Throughout the intercepted recordings, Kropyva and his associates refer to Kravchenko as "Boss" or "Andriyovych." Investigators produced documentation proving Kropyva coordinated Kravchenko's home renovations, bought international flights for him and his spouse, and booked luxury hotel accommodations in Madrid.

Kravchenko forcefully denied all allegations. However, on September 7, 2026, he tendered his resignation, characterizing the step as a political necessity: "I do not want the position of Prosecutor General to be weaponized as a tool in political confrontations." The resignation followed high-level consultations with President Zelenskyy and Davyd Arakhamia, head of the ruling party's parliamentary faction.

Despite the fallout, the Office of the Prosecutor General issued statements pledging cooperation with anti-corruption bodies while simultaneously challenging the procedural legality of certain NABU actions.

IV. Political Entanglements – MPs, the SSU, and the Struggle for Power Davyd Arakhamia – Head of the Ruling Faction Under Fire

Davyd Arakhamia found himself at the epicenter of the chain reaction that culminated in Kravchenko's resignation. Arakhamia was present during the closed-door meeting with the President and the Prosecutor General on September 7. Without his backing, executing high-level leadership shifts within the prosecutor's office would have been politically unfeasible.



Davyd Arakhamia

Allegations concerning Arakhamia date back to 2023, when reports emerged suggesting he might hold a stake in an illicit call center in Tbilisi, Georgia, alongside Georgian opposition figure Giorgi Vashadze. In August 2026, weeks before Operation "Carthage" unfolded, leaks in Ukrainian media signaled that charges against Arakhamia were being prepared. NABU was reportedly conducting searches targeting figures inside the President's inner circle, including former Head of the Presidential Office Andriy Yermak and Arakhamia himself.

While no formal indictment has been issued against him, his persistent proximity to these critical moments keeps him at the center of political fallout.

Oleksandr Kunitsky – A Commission to Eradicate or Protect?

Oleksandr Kunitsky, a Member of Parliament from the "Servant of the People" party, chaired the Temporary Investigative Commission on Cyber Fraud and Financial Pyramids between 2023 and 2024. Although established to dismantle the call center industry, serious questions arose regarding the commission's true objectives over time. Investigative reporters and anti-corruption advocates highlighted that raids carried out under the commission's umbrella appeared designed to eliminate competitors rather than shut down operations. Centers failing to pay protection fees to key political factions were targeted, while protected operations remained untouched.



Oleksandr Kunitsky

Systemic Protection – The SSU and Broader Security Structures

The call center nexus extends far beyond parliament and the prosecutor's office. According to testimonies from detained operators, regional units of the Security Service of Ukraine (SSU) and national police were actively involved. Certain SSU branches collected recurring subscription fees to ensure designated locations remained free from surprise inspections. Operatives named specific officers who received upwards of \$15,000 monthly for providing operational coverage. Particularly revealing context emerged from an incident on Bali, where Ihor Komarov, son of a organized crime figure, named Ukrainian SSU officers who allegedly shielded his network during an interrogation—including Oleksandr Petrovsky (alias "Narik," who reportedly received \$15,000 monthly) and former Head of the Dnipropetrovsk Regional State Administration and current Head of the Odesa Regional Military Administration, Serhiy Lysak.

During the exact week NABU executed Operation "Carthage," an armed standoff occurred in Kyiv between SSU officers and GUR (Military Intelligence) personnel. This friction between Ukraine's principal security services underlines the depth of institutional instability.

Presidential Response – Legislation, Resignations, and Political Containment

President Zelenskyy, who was directly questioned about call centers by journalist Mykhailo Tkach back in 2023, acted swiftly as the scandal exploded:

- Convened an emergency meeting on September 7 with the heads of NABU, SAPO, and Arakhamia.
- Formally accepted Kravchenko's resignation.
- Submitted draft legislation to the Verkhovna Rada proposing prison terms of up to 12 years for call center organizers.

However, analysts and investigative journalists note that the legislative response materialized only after wiretap audio leaked—suggesting a calculated move to reclaim the narrative and limit political damage. Furthermore, reports indicate that elements within the presidential administration and the acting SSU leadership are assembling a political counter-strategy targeting NABU and SAPO.

International Pressure – The Role of the US and EU

Operation "Carthage" did not occur in isolation. During the same week, US presidential envoys Steve Witkoff and Jared Kushner conducted official visits to Kyiv. Analysts assess that the decisive actions taken by NABU and SAPO—institutions backed by Western partners—were bolstered by international oversight. Regardless of internal political maneuvering, the magnitude of the exposure places Kyiv under heightened scrutiny from international allies demanding systemic anti-corruption reforms.

V. Bloody Reckonings – The Monaco Bombing and the Bali Murder

The dirty billions flowing from fraudulent call centers have ignited a cascade of brutal underworld retribution—stretching from the luxury high-rises of Monaco to the exotic beaches of Bali.

The Monaco Bombing

On June 29, 2026, an explosive device packed with nails and screws detonate in the lobby of a luxury residential building in Monaco. The target was Vadym Yermolayev—a Ukrainian businessman, real estate developer from Dnipro, and former Forbes list honoree whose net worth was estimated at \$220 million in 2021.



The blast injured three people: Yermolayev's partner suffered traumatic amputations of both legs, Yermolayev himself sustained severe burns and shrapnel wounds, and his 13-year-old son suffered minor injuries.

Yermolayev, founder of the Alef Corporation, had renounced his Ukrainian citizenship in 2019 in favor of Cypriot nationality. In December 2023, President Zelenskyy placed him under state sanctions after his alcohol distribution businesses in Russian-occupied Crimea were found paying taxes into the Russian state budget.

Investigators determined the assassination attempt was tied directly to call-center operations. Artur Yermolayev, the businessman's eldest son, personally managed a major network of fraudulent call centers that defrauded European victims—primarily in Germany, Estonia, and Ukraine—of over €100 million between 2019 and 2022 through fake cryptocurrency investment schemes. Artur was arrested on a Interpol warrant in Cyprus in late 2025 and subsequently received a suspended sentence alongside extensive asset forfeitures.

The perpetrator was identified as Anastasiya Berezovska, a 39-year-old Ukrainian national who cased the building, disguised herself as a man, and detonated the device remotely. She fled through France to Italy, but on July 6, 2026, her body was discovered outside Kyiv—executed by her handlers to eliminate loose ends. Ukrainian law enforcement subsequently detained two suspects: an active GUR officer and a former SSU operative who had executed multiple wire transfers into Berezovska's accounts. Investigators believe both men were directly involved in orchestrating the attack on Yermolayev.



Anastasiya Berezovska

Bali – Kidnapping, Torture, and Brutal Murder

On February 15, 2026, 28-year-old Ihor Komarov—son of a prominent figure in Dnipro’s criminal underworld—disappeared on the island of Bali, where he had arrived with his girlfriend for a vacation. He was abducted while riding a motorcycle near the village of Jimbaran.

Severe, graphic video recordings soon surfaced online. A bloodied Komarov, with broken legs and severed fingers, pleaded with his family to pay a \$10 million ransom. The abductors claimed Komarov and his associates had stolen that exact sum from them through call-center scams. Under torture, Komarov named several high-ranking Ukrainian officers allegedly protecting his operations, including Oleksandr Petrovsky (alias "Narik").



Despite the ransom being paid, Komarov was executed. On February 26, his severed head was discovered near a river estuary, followed by the recovery of his dismembered remains. Yermak Petrovsky, son of crime boss "Narik," who was accompanying Komarov on Bali, managed to flee the island.

Interpol issued Red Notices for five primary suspects: Ukrainian nationals Denys Halushko, Vasyl Nemesh, and Roman Melnyk; Russian national Nikolay Petrik; and Kazakh national Vladislav Akhanov. Indonesian authorities have detained one suspect to date—a 33-year-old Nigerian national who rented the vehicles used in the abduction. The investigation took a significant turn following intelligence linking Hleb Novostrojnyi, a veteran of the KRAKEN special unit who was present on Bali during the same timeframe, to the operational cell.

The Common Denominator – A War Over Billions

Despite the thousands of miles separating Monaco and Bali, both attacks stem from a single source: the battle for dominance over a call-center industry generating a billion dollars a month. In Monaco, the target was a father financing his son's empire; in Bali, the victim was a son running the operations. In both cases, the syndicates demonstrated total disregard for human life, prompting international law enforcement intervention.

VI. International Response – Interpol, Europol, and Eurojust

As the sheer scope of the syndicate became undeniable, international law enforcement and judicial bodies mobilized to dismantle its global infrastructure.

Interpol – Red Notices and Worldwide Manhunts

Interpol issued Red Notices targeting over a dozen core operatives within the network:

- Artur Yermolayev: Detained in Cyprus in December 2025.
- Anastasiya Berezovska: Red Notice issued on July 3, 2026; later discovered murdered outside Kyiv.
- Bali Murder Perpetrators: Five Red Notices issued for Ukrainian, Russian, and Kazakh nationals, alongside six additional fugitives under active international warrants. In September 2026, Interpol—in direct coordination with the U.S. Drug Enforcement Administration (DEA)—executed a joint crackdown targeting the syndicate's global recruitment channels. Law enforcement conducted 26 raids across recruitment-focused call centers in Ukraine, dismantling their operations and identifying 27 active syndicate participants.

Interpol also served as the primary nexus for international extraditions. In October 2025, Ukrainian authorities extradited a 28-year-old Czech national wanted for leading an international call-center fraud cell back to the Czech Republic.

Europol – Coordinating European Field Operations

Europol spearheaded dozens of cross-border field operations throughout 2025 and 2026:

- March 2026 – Operation "Scammer" (Jointly with Latvia): Exposed two Ukrainian nationals operating a dedicated call center that defrauded at least 20 Latvian victims, generating losses exceeding €300,000.
- June 2026 – Network Dismantling: Shut down an Albanian-linked fraud structure that extracted over €50 million from targets across Europe.
- October 2024 – Joint Operation with the Czech Republic: Dismantled a call-center syndicate targeting EU citizens, culminating in the arrest of three foreign nationals in Ukraine's Kirovohrad Region.

Eurojust – Judicial Coordination and Asset Seizures

Eurojust provided judicial logistics, legal frameworks, and coordination for Joint Investigation Teams (JITs) targeting the network:

- December 2025 – Multi-City Sweep (Dnipro, Ivano-Frankivsk, Kyiv): Operatives executed 72 search warrants and 12 arrests, identifying 45 key suspects. The cell defrauded over 400 victims of more than €10 million. The facility employed roughly 100 operators recruited from the Czech Republic, Latvia, and Lithuania. Workers were offered a 7% commission and performance bonuses for theft exceeding €100,000, though bonuses were routinely withheld.
- May 2026 – Kharkiv Network Dismantling: Authorities conducted 14 raids, apprehending four ringleaders and seizing 49 mobile devices, computer equipment, and luxury vehicles.
- February 2026 – Dnipro Operation: Law enforcement dismantled a major call center targeting victims via fraudulent cryptocurrency platforms, resulting in 11 arrests. Victims in Latvia and Lithuania suffered losses exceeding €160,000. The operation encompassed 32 search warrants, seizing €400,000 in physical cash, cold cryptocurrency storage wallets, and high-end vehicles.

UN Human Rights Assessment

The Office of the United Nations High Commissioner for Human Rights (OHCHR) formally highlighted systemic human rights violations stemming from industrial-scale cyber fraud networks, emphasizing the global, organized nature of human exploitation and forced labor within illicit call-center structures.

VII. Human Tragedies – Victims Reduced to Statistics

Behind the staggering figures and technical architecture lies the human cost: thousands of individuals stripped of their life savings, homes, and dignity.

The Story of Helena (68, Kraków, Poland)

Helena received an urgent call from an operator posing as a bank security officer, claiming unauthorized individuals were attempting to secure a high-value loan using her personal data. Coerced into "protecting" her assets, she transferred 120,000 PLN (€28,000) to a designated "safe account." The funds vanished immediately.

The Story of Klaus (54, Munich, Germany)

Klaus was targeted by a cold caller impersonating a federal prosecutor, who claimed he was under immediate threat of arrest for alleged financial crimes. In a state of panic, Klaus liquidated his apartment and wired €340,000 to a "court-controlled vault." His life savings were wiped out.

According to Berlin authorities, Ukrainian syndicates were responsible for 40% of all fraudulent calls registered in Germany in 2025 alone, extracting an estimated €800 million annually from German citizens.

In Lviv, law enforcement dismantled a dedicated center that defrauded 114 EU citizens—including 51 Italian and 50 German nationals. Operators impersonated representatives of "Olimp," a fictitious legal recovery firm promising to claw back capital previously lost to fraudulent trading platforms,

deliberately exploiting individuals who had already been victimized.

The Secondary Recovery Scam

A major revenue stream across these operations involved targeting individuals who were previously defrauded. Operators re-contacted targets under the guise of international courts, tax authorities, or asset-recovery firms, convincing them to pay upfront legal or escrow fees to retrieve their stolen funds. Once paid, the secondary fees disappeared alongside the original losses.

Human Trafficking and Forced Labor Under the Cover of Call Centers

In January 2026, Polish law enforcement dismantled a major human trafficking ring in Warsaw operating under the facade of call-center recruitment. Police arrested 22 individuals, including 12 Ukrainian nationals.

Anastasiya, an 18-year-old Ukrainian national, responded to a job posting on Telegram. Upon arriving at a residential compound in Warsaw's Ursynów district, she and dozens of others were stripped of personal documents, held under strict physical confinement, and intimidated using graphic violence videos. Confined workers were forced to map international illicit drug networks online. Anastasiya spent three weeks in captivity before another detainee escaped and alerted emergency services (112). Police liberated 22 Ukrainian nationals from the site. The organizers face up to 25 years in prison.

The Scale of Financial Damage in Poland

During the first half of 2026, Polish police registered 8,451 criminal offenses committed by foreign nationals, with the majority attributed to Ukrainian citizens operating within organized structures. Investigations by Poland's Central Cybercrime Bureau (CBZC) revealed staggering figures:

- Primary Cybercase A: Identified 15,000 individual victims with cumulative losses exceeding 750 million PLN (~€175 million).
- Primary Cybercase B: Documented 1,500 victims with verified losses of 75 million PLN (~€17.5 million).

Industrial Capacity

In March 2026, law enforcement in Ukraine's Dnipropetrovsk region dismantled a single syndicate employing over 1,500 active operators. By August 2026, Ukrainian police executed 411 simultaneous search warrants nationwide, shuttering 94 illicit call centers containing 1,794 fully equipped operator workstations.

The true global financial toll remains fundamentally unquantifiable. A significant percentage of victims never report their losses to law enforcement due to psychological shock, social stigma, or the conviction that international legal remedies are ineffective.

VIII. The Price of Billions – Questions of Accountability and Gratitude

A Nation Defrauding Its Benefactors

While the Ukrainian military fights on the frontlines and Western allies— primarily Poland, Germany, and the United States—pour billions of dollars into sustaining the Ukrainian state, a shadow war is being waged behind the scenes. Poland, which allocated over 100 billion PLN in aid to Ukraine between 2022 and 2023, continues to finance critical elements of Ukraine's infrastructure. In 2026 alone, maintaining the Starlink satellite system costs Polish taxpayers 168 million PLN. Poland has provided Ukraine with over 29,000 satellite terminals and continues to fund their operations, while over 90% of Western aid flows through the logistics hub in Jasionka.

Polish taxpayers also subsidize benefits for Ukrainian refugees—with the 2026 Assistance Fund allocating 1.08 billion PLN in direct support.

Meanwhile, elements within the very population sustained by the generosity of Polish, German, and American citizens are orchestrating large-scale fraud operations targeting their benefactors. Ukrainian nationals constitute the core of organizers and operators running fraudulent call centers on Polish territory.

Is Zelenskyy Blind and Deaf?

President Zelenskyy has repeatedly made public pledges to eradicate corruption. When questioned about call centers by journalist Mykhailo Tkach in 2023, the President assured the public that law enforcement was handling the issue. However, Operation "Carthage" revealed that the protective apparatus shielding these call centers reached the highest levels of the prosecutor's office. Prosecutor General Ruslan Kravchenko— appointed by Zelenskyy—appears in wiretapped recordings as "The Boss," whom subordinates explicitly addressed saying: "You're covering for me. That's why everybody knows." Furthermore, the investigation exposed systemic hypocrisy: call centers aligned with prosecutorial interests received total immunity, while unaligned facilities were raided to demonstrate fake "progress" in anti-corruption efforts demanded by the presidency. In intercepted audio, Kropyva can be heard inquiring about the ownership of specific call centers; upon learning a target center was "unaffiliated," prosecutorial raids were executed the following day. The President demanded results, but his own prosecutorial apparatus shielded its protected operations while raiding rivals to satisfy quotas.

The Inner Circle – High-Level Corruption

The call-center scandal is not an isolated incident within the presidential administration. In May 2026, Andriy Yermak, former Head of the Presidential Office, was indicted for participating in an organized criminal enterprise and laundering 460 million UAH (~\$11.2 million) linked to luxury real estate developments outside Kyiv. Yermak resigned from his post in November 2025, one day after search warrants were executed at his properties.

Similarly, an investigation into state nuclear energy operator Energoatom uncovered a systemic kickback scheme where contractors paid 10–15% skim off contract values. Illicit proceeds—totaling roughly \$100 million—were laundered through a covert back-office apparatus. Nine primary suspects face formal charges, including Timur Mindich—a close Zelenskyy associate often characterized as his "financial custodian"—who is currently hiding in Israel fighting extradition, former Deputy Prime Minister Oleksiy Chernyshov, and former Energy Minister Herman Halushchenko.

Calculation Replacing Gratitude

While soldiers perish on the frontlines and Ukrainian cities endure relentless bombardment, Western allies receive fraud in return. Poland spent billions in assistance, yet its citizens face daily extortion by Ukrainian nationals operating from Ukrainian territory under the protection of a prosecutorial system overseen by the presidency.

"Is this fair?"—this question is increasingly raised by ordinary Polish, German, Czech, and American citizens. In 2026, Poland's state budget allocates over a billion PLN to Ukrainian assistance, while a single cybercrime investigation into local call centers revealed verified losses of 75 million PLN inflicted on Polish citizens—capital that could have funded local healthcare, schools, or pensions.

Unanswered Questions

- Was Zelenskyy genuinely unaware of the systemic criminal activity taking place inside state institutions he directly leads?
- Was he truly blind to years of investigative journalism sounding the alarm?
- As suggested by the Mindich wiretaps—where top aides discuss embezzled funds while referencing the moniker "Vova"—was he merely aware, or jointly responsible?
- Why does he continue to retain key figures who belong behind bars? As Newsweek observed, cascading corruption scandals surrounding the presidency leave Zelenskyy in his weakest political position since the start of the full-scale invasion.

Conclusion – Will "Carthage" Be Destroyed?

Operation "Carthage" was unprecedented. NABU and SAPO exposed a criminal organization that, at its peak, controlled roughly 500 call centers. Over the past 12 months, law enforcement executed over 1,050 search warrants, shuttering approximately 340 illicit operations containing over 5,000 operator workstations.

As investigator Pavlo Demchuk emphasized: "This is merely the beginning of the public phase of the pre-trial investigation." If current charges are proven in court, he added, it will expose profound structural failure across the entire prosecutorial system.

Yet critical questions remain unanswered. Are these high-profile arrests genuine accountability, or merely political sacrifices designed to placate Western donors? Will the investigation reach

higher—targeting those who knew for years but remained silent? Is a president who, as recently as July 2026, signed legislation restricting the investigative authority of NABU and SAPO, genuinely prepared to prosecute his inner circle?

Zelenskyy remains caught between a rock and a hard place: Western partners demanding results on one side, and his internal political network on the other. Former Defense Minister Mykhailo Fedorov stated directly: "The President must answer whether he was aware of potential corruption within his immediate environment. It is his direct responsibility to inform the public whether he was aware or not."

Meanwhile, media leaks continue to compromise state credibility. According to Ukrainska Pravda, Kravchenko compiled intelligence dossiers on NABU investigators and their immediate families prior to his resignation. Simultaneously, the President's September 3, 2026 legislative draft proposing harsher penalties for call-center organizers—submitted one day prior to Operation "Carthage"—was widely criticized by analysts as a performative gesture targeting Western audiences.

Behind the political maneuvering and economic statistics stand real human beings—pensioners, families, and ordinary citizens stripped of their life savings.

Ancient Carthage had to be razed to the ground for Rome to secure its future. Today, Ukraine's "Carthage"—the billion-dollar call-center empire— faces the prospect of collapse. Dismantling an infrastructure this deeply entrenched requires more than courageous investigators and journalists; it demands uncompromising political will and systemic institutional reform.

Whether a nation fighting for its survival on the frontlines possesses the internal strength to simultaneously eradicate corruption within its own ranks remains to be seen. The answer depends not just on NABU and SAPO, but on whether the Ukrainian state and its leadership have the courage to face the truth.

Time will tell. But the clock is ticking.

This investigative report was compiled based on investigative materials from Ukrainska Pravda, official intelligence and case files from NABU, SAPO, Interpol, Europol, the Global Initiative Against Transnational Organized Crime (GI-TOC), alongside verified media reporting across Poland, Germany, the United Kingdom, and Ukraine.

Editorial update — information checked on 30 October 2026

This update separates information supported by the institutional statements consulted from claims in the reprinted material above. The operations described concern distinct investigations: they must not automatically be treated as a single organisation or their results added together.

Carthage: what NABU actually reports

On 5 September 2026, NABU and SAPO described an organisation allegedly led by a department head at the Prosecutor General's Office. Investigators said it was established in mid-2025 and involved serving prosecutors and informal associates. The alleged arrangement involved bribes in exchange for non-interference with fraudulent call centres targeting Ukrainians and foreign nationals. Five participants had been exposed at that stage. These are investigative allegations, not a final conviction. [3]

NABU reported over UAH 20 million spent on real estate, jewellery and other property. The alleged leader was accused of laundering property with a minimum market value exceeding UAH 12 million, including by registering it in other people's names. Separately, over UAH 10 million was reportedly deposited into associates' bank accounts disguised as business income. These figures describe particular assets and flows; they cannot simply be added together or used to calculate the entire fraud industry's monthly turnover. [3]

On 22 October 2026, NABU announced another suspect in Operation Carthage: a former department head at the Prosecutor General's Office. Investigators allege that he communicated directly with illegal call-centre representatives, systematically collected bribes, provided protection and recruited others. The statement put the total documented illicit benefit at more than UAH 1 billion. The investigation remains ongoing. [4]

Dnipro and Kharkiv: two documented investigations

On 23 February 2026, Eurojust described joint Latvian, Lithuanian and Ukrainian action against a fraudulent call centre operating through three offices in Dnipro. The scheme involved fake cryptocurrency investments, subsequent demands for purported legal assistance to recover losses, and remote-access software to reach victims' funds. Initial findings identified at least nine victims in Latvia and Lithuania with losses exceeding EUR 160,000. On 17 February, authorities arrested 11 people and searched 32 locations, seizing, among other items, EUR 400,000 in cash, two cryptocurrency wallets and eight luxury cars. The seized amount is not the same measure as identified victim losses. [5]

In a separate case reported on 29 May 2026, cooperation between Latvia and Ukraine closed a call centre in Kharkiv. According to Eurojust, operators targeted older people who had already suffered fraud and demanded additional payments while pretending to recover their money. They used misleading investment offers, fabricated profit reports and credit agreements created without victims' knowledge or consent. The action on 26 May produced four arrests and 14 searches. Eurojust also described surveillance, access controls and employee polygraph screening. This is a documented example of repeat victimisation, not proof that every call centre uses identical methods. [6]

Interpol: global operations, deepfakes and asset interception

On 9 July 2026, Interpol reported results from First Light 2026, conducted from 15 January to 30 April across 97 countries and territories. It reported 5,811 arrests, over 142,000 identified victims and USD 293 million in intercepted illicit assets. Authorities blocked 31,014 bank accounts; Europol supported the operation. These are global anti-fraud results, not the balance sheet of Ukraine's Carthage investigation or confirmation of every case or name in the reprint. [7]

On 19 October 2026, Interpol launched an awareness campaign on AI deepfake scams. Small amounts of publicly available content can help criminals imitate a face or voice and impersonate a relative, partner or company representative. Warning signs include unsolicited contact, urgency, emotional manipulation and unusual payment requests. Interpol recommends verifying identity through an independently known channel, family safe words, two-factor authentication and additional transaction checks in businesses. Anyone who has sent money should promptly contact their bank and police. This is global threat guidance, not an attribution of these techniques to specific people named in the article. [8]

In information released on 30 June 2025, Interpol said trafficking victims exploited in scam centres had been identified from 66 countries as of March 2025. It distinguished people coerced into criminal work from financial fraud victims, and noted that not every scam-centre worker has been trafficked. Expansion beyond Southeast Asia demonstrates the international character of the problem; it does not establish trafficking in every European office discussed here. Interpol's March 2026 threat assessment also describes links between financial fraud, cybercrime and other forms of organised crime. [9] [11]

A Red Notice is not an international arrest warrant

Interpol explains that a Red Notice requests law enforcement to locate and provisionally arrest someone pending extradition, surrender or similar proceedings, on an underlying national legal basis. It is not itself an international arrest warrant; each country applies its own law. The person is wanted by a country or an eligible tribunal, not prosecuted by Interpol. This explains the procedure; it does not establish that a particular notice exists for anyone named in the reprint. [10]

Sources and further information

1. Oryginalna publikacja TRUTH magazine na LinkedIn / Original TRUTH magazine publication
<https://www.linkedin.com/feed/update/urn:li:ugcPost:7503522512136200192/>

2. Przekazany plik PDF — pełna kopia źródła / Supplied PDF — full source copy
<https://truthmagazine.eu/downloads/articles/fraud-imperium-source.pdf>

3. NABU, 05.09.2026 — ochrona call center i pranie pieniędzy / protection of call centres and money laundering
<https://nabu.gov.ua/en/news/kryshuvannia-kol-tcentriv-ta-vidmyvannia-mayina-vykryto-zlochynnu-organizatsiiu-na-choli-z-posadovtsem-ofisu-genprokurora/>

4. NABU, 22.10.2026 — Operation Carthage: new suspect
<https://nabu.gov.ua/en/news/operatsiia-karfagen-nova-pidozra/>

5. Eurojust, 23.02.2026 — 11 arrests during actions against fraudulent call centre (Dnipro)
<https://www.eurojust.europa.eu/news/11-arrests-during-actions-against-fraudulent-call-centre>
 6. Eurojust, 29.05.2026 — Scam call centre shut down thanks to Eurojust-supported investigation (Kharkiv)
<https://www.eurojust.europa.eu/news/scam-call-centre-shut-down-thanks-eurojust-supported-investigation>
 7. INTERPOL, 09.07.2026 — First Light 2026: arrests and intercepted assets (global operation)
<https://www.interpol.int/en/News-and-Events/News/2026/Over-5-800-arrests-USD-293-million-intercepted-in-global-fraud-bust>
 8. INTERPOL, 19.10.2026 — public awareness campaign on AI deepfake scams
<https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-launches-public-awareness-campaign-highlighting-risk-of-AI-deepfake-scams>
 9. INTERPOL, 30.06.2025 — globalization of scam centres and trafficking (global context)
<https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres>
 10. INTERPOL — Red Notices: meaning, legal limits and presumption of innocence
<https://www.interpol.int/en/How-we-work/Notices/Red-Notices>
 11. INTERPOL, 16.03.2026 — Global Financial Fraud Threat Assessment 2026
<https://www.interpol.int/en/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>
- Online version: <https://truthmagazine.eu/publikacje/fraud-imperium/>