GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

KYIV CALLING

THE SCAM CALL CENTRE PHENOMENON IN UKRAINE

APRIL 2026

ACKNOWLEDGEMENTS

This report was authored by the Global Initiative Against Transnational Organized Crime (GI-TOC)'s Eurasia Observatory, the successor to the Observatory of Illicit Markets and the Conflict in Ukraine, which was established in 2022. The observatory provides timely, granular analysis on organized crime, illicit markets and the enabling conditions in the Eurasia region, with a particular focus on shifts driven by the war in Ukraine.

Cover: © *David Trood/DigitalVision via Getty Images, Unsplash*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland

www.globalinitiative.net

CONTENTS

Executive summary **1**

A note on methodology 2

Key points 3

Introduction: the scam phenomenon **4**

From skimming to scamming 5

The criminal ecosystem: five characteristics **8**

Open but secure 8

Highly networked, criminally connected 12

Officially protected 14

Global reach 16

Tech-enabled 18

Life inside a call centre **19**

Getting in 19

The job 20

Getting out 20

Future trends: decline or adaptation? **22**

Doubling down on the global market 23

From business centre to remote work? 23

AI and crime as a service 24

Recommendations **26**

Close the shop window 26

Take down networks, not call centres 27

Break the shield of protection 28

Streamline international investigations 29

Maximize defensive AI with a political strategy and user responsibility 30

Notes 31

EXECUTIVE SUMMARY

Scam call centres have become an extremely lucrative and highly networked illicit activity in Ukraine, second only to economic crime by some estimates, and outstripping drugs.[1] The operations of scam call centres include romance fraud, investment fraud, impostor fraud (impersonating bank or government officials) and numerous other ways of taking money from trusting victims. The role of social engineering in this kind of fraud cannot be underestimated – it is what differentiates it from 'hands-off' forms of fraud such as spam or ATM skimming, and often brings greater rewards. According to research by the Ukrainian Interbank Payment Systems Member Association (EMA), an anti-fraud organization, the average loss through socially engineered fraud in Ukraine in September 2024 was €202, compared to €15 for online scams.[2] Today, frauds such as ATM skimming have largely fallen by the wayside in Ukraine, with socially engineered fraud in the ascendant, reflecting a global trend.[3]

How did this curiously hybrid form of crime, which combines internet communication technologies and cryptocurrency laundering with phone calls and social engineering, accelerate so quickly? What have been the internal and external factors? And how has the Russo-Ukrainian war shaped the development of this illicit industry?

This report traces the regional evolution of scam call centres over the two decades since they first emerged in Georgia (which imported the idea from Israel). Ukraine emerged as a hotspot after the Russian-backed insurgency in the Donbas and the Russian annexation of Crimea in 2014, with Dnipro and Kyiv becoming national powerhouses.

Amid a broader shift from kinetic crime (involving physical force or violence) to fraud after the full-scale Russian invasion in 2022, scam call centres today can be found in each of Ukraine's 24 oblasts (regions), including the Russian-occupied territories. Numbers are difficult to verify but the size of the economy is huge: by one calculation, about 60 000 Ukrainians work in scam call centres – two-thirds the number of those employed in the legal banking sector.[4] Overall, judging from figures provided, it is plausible that Ukraine's scam call centre economy can generate as much as US$1 billion a month, though overheads are considerable.[5] Most of the profit is taken by the bosses, while those who work as low-level scammers rarely get rich, despite the fantastic promises made to them on social media platforms and job websites.

The industry is highly consolidated. Just three networks reportedly manage most scam call centres, with significant involvement of 'traditional' organized crime.[6] These networks often benefit from protection by law enforcement, rendering them immune from prosecution and ensuring any that are apprehended can usually set up shop again without much disruption.[7]

As it has matured, the illicit industry has evolved. From initially targeting Russians and Ukrainians it has now gone global, with victims recorded in at least 29 countries.[8] Advertisements in Russian and Ukrainian have started to appear elsewhere in Europe, suggesting that scam call centres with ties to Ukraine have spread and are recruiting from the Ukrainian refugee population (which has also been targeted by scammers). Technology, particularly artificial intelligence (AI) and crime as a service, is radically expanding the scale, capabilities and sophistication of scammers.

Ukraine's scam call centres have developed to such an extent that a Kyiv official said it was important to prevent the country becoming a global hotspot of fraud rivalling the Golden Triangle in South East Asia.[9] A more pessimistic analysis may conclude that Ukraine has already reached this status, making action even more urgent. At the time of writing, the green shoots of progress were in evidence. At the behest of the new prosecutor general, law enforcement embarked on a crackdown in July 2025, shutting 25 call centres in Dnipro alone.[10] The pace continued throughout the second half of the year, with dozens more call centres shut down.[11] In December, Ukraine, together with European law enforcement partners, dismantled a transnational network with call centres in Kyiv, Dnipro and Ivano-Frankivsk that had scammed 47 Europeans of almost a million euros.[12]

But as this report details, eradicating the scam call centre phenomenon will require more than raids and arrests, not least due to the revolutionary impact of AI and crime as a service, which may fundamentally upend the current model. In future, the work of scam call centres may no longer be the preserve of large, heavily capitalized operations, but open to anyone with the will and a few thousand dollars to set up their own venture. This could lead to an exponential increase in the number of scammers and scams, with geography, time and language no barrier.

A note on methodology

Research for this report adopted a mixed-methods approach. Interviews were conducted with four former employees of scam call centres, as well as an MP who had worked on an official commission investigating the scam call centre phenomenon and a representative of EMA, a Ukrainian banking association whose mandate includes tackling fraud. Further background was provided from the GI-TOC's interviews in the past with law enforcement, activists and journalists regarding scam call centres in the cities of Dnipro and Odesa. Interviews were conducted both in person and remotely, as security dictated. These interviews were complemented by extensive open-source analysis of Ukrainian, Russian and English sources.

As the research highlighted, the scam call centre ecosystem is shrouded in secrecy, and while every effort was made to triangulate information, corroboration was often challenging. This was particularly the case in relation to the political protection of scam call centres. Legal cases against corrupt law enforcement officials are largely absent, aside from a few cases, but the circumstantial evidence of call centres continuing to operate after raids, testimony of former call centre employees, and lack of progress in some prosecutions are suggestive of the climate of political protection. The political overlay of the Russo–Ukrainian War must also be taken into account, especially when reading Russian claims of Ukrainian scamming, given that Moscow has clear interests in amplifying the threat of Ukrainian scam call centres and the claim of protection.

As such, the analysis presented in this report is designed to provide a working model of a secretive industry, as opposed to presenting a definitive statement. More information is required to provide greater clarity and detail regarding the diversity and intricacy of such operations, particularly as they

relate to market consolidation and the involvement of 'traditional' criminal elements, use of advanced technology, and role of corrupt officials in facilitating the industry.

Key points

To help inform a comprehensive strategy, this report details the five key characteristics of scam call centres in Ukraine and makes recommendations for each:

- **Open but secure.** Scam call centres advertise openly for staff and predominately operate from well-secured city centre buildings. Recommendations: Improve screening of job websites and social media, including sharing intelligence with law enforcement; raise public awareness of the gap between promise and reality when it comes to call centre pay and working conditions; incentivize landlords to stop scammers renting office space. Legislation should be developed to close legal loopholes.
- **Highly networked, criminally connected.** Owners have stakes in many call centres and are often linked to organized crime. Recommendations: Make sure fraud cases end up on the right law enforcement desk; build cases against networks, not individual call centres; revisit recommendations by the temporary investigative commission established by the Verkhovna Rada (Ukraine's parliament) to introduce new articles to the criminal code on electronic communication fraud, and other applicable legislation.
- **Officially protected.** Some corrupt elements in law enforcement are alleged to provide protection for scam call centres. Recommendations: Break the shield of protection by reviving political efforts to focus on call centres. Western partners must also increase pressure on their Ukrainian counterparts, making clear that protection of call centres harming European citizens is unacceptable.
- **Global reach.** Target countries of scam call centres are spread across the Global North. Recommendations: Develop streamlined international protocols to investigate international fraud. This is the only way to keep pace with the exponential increase of fraud and lower the resource cost of transnational investigations.
- **Tech-enabled.** Scam call centres make extensive use of technology. Recommendations: Tech will be at the front line of responses to scams, but by itself it is not sufficient. The state should develop a comprehensive anti-scam strategy that coordinates defensive AI, holds service providers to account and emphasizes the need for personal cybersecurity responsibility.

INTRODUCTION: THE SCAM PHENOMENON

In the mid-20th century, most fraud took place face to face, but the rise of communications technology dramatically changed the fraud landscape. By the 1970s, the telephone had become a key weapon to conduct far-reaching fraud at scale, from telemarketers to the 'boiler rooms' – call centres that sold worthless securities to unsuspecting investors – depicted in the movie *The Wolf of Wall Street*.[13]

Another cycle of evolution began with the rise of the internet, especially the enabling capacity offered by voice-over-internet protocol (VoIP) telephony, which dramatically lowered the cost of calling victims overseas; spam email; and the ease of making international money transfers using online payment systems (such as PayPal).[14] Now scammers armed with nothing more than a computer and a database of numbers could extract money from anyone, anywhere.

While solo scammers could and did work profitably, the scam call centre – in various sizes, shapes and forms – allowed for organization and therefore economies of scale, greater reach and a laboratory for innovation, especially in the field of tactics and technology concerning the three core scam themes: investment, romance and impostor fraud. Across the world, diverse scam ecosystems have emerged, all with distinctive traits regarding how they employ and manage people, and the organizational structure of the groups involved.

This report focuses on the development of an ecosystem that originated in Israel before moving to Georgia and thence to the broader region, including Ukraine.

What are scam call centres?

Scam call centres originated with the telephone as their primary instrument but they have become much more sophisticated. Deepfakes, money laundering and specialized software have added tools to the scammers' arsenal, but their defining characteristic is social engineering: scammers create a relationship with victims that aims to make them perform a certain action and/or part with sensitive information or money.

This report focuses on scams that involve personalized social engineering rather than anonymous and automated scams such as mass phishing (although phishing can be a component of scam call centre activities). The centrality of this human relationship – based on fear, greed or need – unites the diverse range of criminal acts perpetrated by scam call centres. ■

From skimming to scamming

Scam call centres based on foreign exchange investment scams (so-called 'binary options') became prominent in Israel in the mid-2000s before being banned in 2017.[15] By 2008, however, their ideas and methods – the structure, schemes, scripts, technology and money laundering know-how – had already migrated to Georgia, and later Ukraine.[16]

In the mid-2010s, scam call centres were already prevalent in Ukraine, but the Milton Group took the principle to an industrial level. International, highly organized and extremely profitable, the Kyiv branch of the network targeted victims all over the world (some lost more than US$200 000) and had alleged links to call centres in Albania, North Macedonia and Georgia.[17] (The Milton Group CEO denied defrauding anyone, claiming clients did not understand the nature of the investments.[18])

Exposure of the Milton Group by the Organized Crime and Corruption Reporting Project (OCCRP) in 2020 did little to dampen the growth of scam call centres, also known as *ofisy* (offices). By the time of Russia's invasion in February 2022, they had become an established part of the criminal landscape in Ukraine, and *ofisniki* (office workers) were a recognized criminal group with a distinctive image and traits.

The eastern city of Dnipro quickly became a hotspot for this form of commercially organized fraud, leading the deputy chairperson of Sberbank, the largest Russian bank, to label it 'the capital of telephone fraud' in 2021.[19] According to a woman who worked in a call centre there, 'in Dnipro there are more "offices" than cafes'.[20] Scam call centres also began to spread more widely, and many were set up by detainees in pre-trial detention centres.[21]

Russia's full-scale invasion had a direct impact on scamming in Ukraine. After a period in which scams fell to zero, scammers adapted to the new reality and levels of activity returned to normal.[22] In 2022, there were almost 90 000 reports of online fraud, with an estimated €25 million in losses, and these probably represent only a fraction of the total.[23] Interestingly, there was a decline in more physical forms of scamming due to the new context of conflict and martial law. According to an EMA representative:

> Prior to the invasion, criminal groups from abroad specializing in installing ATM skimmers regularly operated in Ukraine. Domestic groups also engaged in ATM skimming, but they too have largely abandoned this activity, as increased city patrols and closer scrutiny of suspicious behaviour make the risk of being caught much higher. While skimming and ATM fraud were once a significant problem, today such cases are extremely rare.[24]

The online sphere also enabled scammers to take advantage of new opportunities presented by the war, including scams involving aid from international organizations, fake charity and fundraising schemes, fake purchases of military gear and medicine, and fake transport schemes. Scammers also began soliciting 'rescue fees' from people whose relatives had been captured by Russians or disappeared in the occupied territories, and concocted ways to defraud the families of dead soldiers.[25] Scammers also created fake crowdfunding campaigns for the purchase of military equipment.[26] Pensioners were called by fraudsters posing as law enforcement officers who said they had been accused of treason and demanded money to 'mitigate the situation'.[27] Scammers even harvested the data of Ukrainian refugees in order to extort them abroad.[28] Surging interest in cryptocurrencies among the civilian population also created new opportunities.[29]

Russia represented a lucrative and politically amenable target. Russians had been scammed since at least 2014, but now 'patriotic scamming' massively ramped up as scammers took the chance to 'whitewash' their reputations, in the opinion of one commentator.[30] Former scam call centre employees said they had fewer moral and ethical qualms when targeting 'the enemy'.

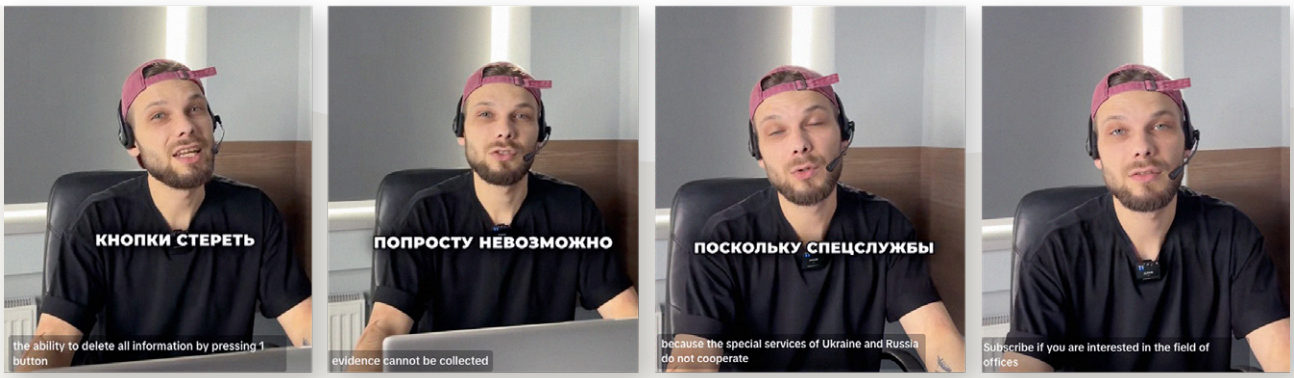
The volume of these calls was enormous: in February 2024, a Russian official estimated that 8 million scam calls were being made to Russia every day, with a further 7 million through other communication channels – mostly from Ukraine.[31] This was up from an estimated 300 000 calls a month before the invasion, representing approximately an 800-fold increase in scam calls.[32] By impersonating officials from Sberbank or Russia's Ministry of Internal Affairs, Ukrainian scammers often persuaded victims to go to extraordinary lengths to part with their money: one former scammer recalled a case in which a Russian national had driven a tractor to an ATM at 3 a.m. to wire money.[33]

Scams targeting Russians were also relatively risk-free, given the lack of law enforcement cooperation between Russia and Ukraine. As an EMA representative put it, 'Smart criminals exploit geopolitics and follow the principle of "Don't dirty where you live and work," targeting bank customers abroad rather than at home. Especially in times of war or geopolitical conflict, they focus on victims in countries from which complaints cannot realistically be filed and criminal cases cannot be opened.'[34]

But it was not only money Ukrainian scammers sought. In a single week in mid-2023, more than 30 arson attacks, by perpetrators ranging from young people to pensioners, targeted military registration and enlistment offices in Russia. It emerged that many had been socially engineered by phone scammers, who had convinced some of the arsonists that they had been recruited by an agent of the Federal Security Service of the Russian Federation (FSB) for a special operation.[35] These attacks were widely seen in Russia as the efforts of Ukrainian scammers, although concrete evidence has yet to be produced to confirm these claims. In December 2024, President Vladimir Putin spoke out about the impact of Ukrainian call centres on Russia, saying they had been 'elevated to the rank of state policy, this is one of the lines of attack on you and me, on our population'.[36]

But scammers do not abide by principles and Ukrainians were fair game as well. According to a media report citing sources in Ukraine's Cyber Police, scam calls to Russia in 2022 and 2023 were never more than 10–15 per cent of the total.[37] And it appeared that scammers were deliberately targeting the most vulnerable: according to the Cyber Police, internally displaced people were the main victims in 2023.[38]

According to an MP who worked on a temporary investigative commission established in 2023 by the Verkhovna Rada to look into possible fraud by scam call centres in Ukraine, 'Some said they were



A TikTok ad for scam call centres seeks to quell fears of prosecution by explaining that Russian and Ukrainian law enforcement officials do not cooperate with each other. *Photos: Screengrabs from @scamline.office on TikTok, https://www.tiktok.com/@scamline.office/video/7507639524017753400*

working against the Russians when in fact the majority of their "clients" were in Ukraine or the EU. In reality, a call centre doesn't give a shit who it profits from.'[39]

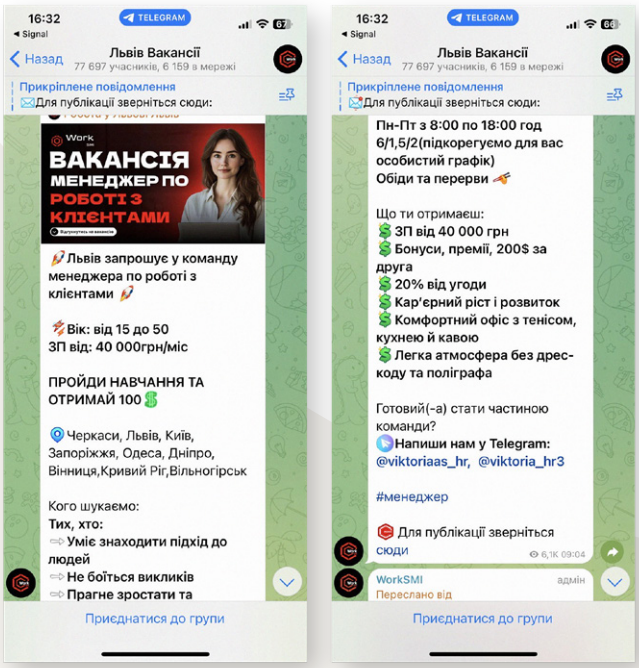
The truth was that call centres were now far too lucrative to be reined in by ideology, and expansion into new markets was only natural. Social engineering had taken fraud to a new level: before the invasion, the average fraudulent transaction for a simple online scam was just €12, compared to €143 for socially engineered fraud. By September 2024, the crimes were worth €15 and €212, respectively. Put simply, the human connection was worth the effort, by a factor of 14.[40]

With so much money to be made, scam call centres proliferated. In mid-2023, there were an estimated 1 000–2 000 call centres in Ukraine, though a subsequent crackdown reportedly reduced this figure by a third.[41] According to one analysis, at their peak as many people worked in scam call centres as in Ukraine's banking sector, although the actual proportion appears to be closer to two-thirds.[42]

Even after the crackdown, Dnipro and Kyiv remained epicentres of fraud – as of late 2024, 30 000 people were reportedy working in 'offices' in Dnipro alone – but the scam call centre phenomenon had already metastasized throughout the country.[43] Organized crime migrated away from the 'hot' areas of eastern Ukraine after the invasion, opening new scam call centres in safer areas such as Odesa, Zhytomyr, Vinnytsia, Transcarpathia and Lviv.[44]

There have been media reports of scam call centres operating in each of Ukraine's 24 oblasts since the invasion, including in the occupied territories, where despite their best efforts to masquerade as Russian, the context of the war could sometimes catch scammers out.[45] A lawyer in the occupied territories advised victims to ask, 'Whose Lugansk is it – Ukrainian or Russian?', using the Russian rendering of 'Luhansk' to provoke a reaction that would reveal the scammer's Ukrainian identity.[46]

The size of a scam call centre depends on its location – the more populous an area, the more chance of attracting employees, and the bigger the call centre. In major cities such as Kyiv, Dnipro, Odesa and Lviv, scam call centres can number 250–300 people working simultaneously. Revenues can be vast, especially for investment scams. According to the MP who worked on the commission, a medium-size 'office' makes US$1 million a month and a large one up to US$3 million.[47] Assuming that medium is the average, and estimating 1 000 such centres in Ukraine after the crackdown, this represents a potential market revenue of US$1 billion a month, although the overheads are considerable, including office space, headcount, tech and protection payments.



A June 2025 Telegram advert for a scam call centre role in Lviv.

The upshot of this surge has been a transformation in the way fraud is conducted in Ukraine and how organized crime functions more generally. Echoing a global trend, scam call centres in Ukraine are now arguably a more profitable illicit venture than drugs.[48] And criminals in other illicit industries – as well as corrupt officials – have taken note.

THE CRIMINAL ECOSYSTEM: FIVE CHARACTERISTICS

Five key traits enable the scam call centre ecosystem in Ukraine to survive and thrive:

- Open but secure
- Highly networked, criminally connected
- Officially protected
- Global reach
- Tech-enabled

Without understanding these five traits, efforts to dismantle the ecosystem – as opposed to individual takedowns of call centres – will largely be frustrated.

Open but secure

One of the most striking facets of scam call centres in Ukraine is their visibility. Recruitment combines physical advertisements such as posters and fliers, online adverts on platforms including the job-search websites work.ua, olx.ua and robota.ua, and open Telegram channels looking for 'client' and 'retention managers', or even 'baristas' or 'barbers'. ('By now everyone knows what those really mean,' said a scam call centre's former human resources (HR) employee.)[49] Many call centres also advertise on TikTok, which makes them relatively easy to locate (see box: Geolocating a call centre).[50]

Many adverts for scam call centres appear to resemble those of legitimate business call centres, although the offered salaries are higher and communication after the initial contact is through Telegram. Another differentiating factor is that wages are paid weekly.[51]

Scam call centres are hardly masters of disguise. Scammers do not use basements or compounds in remote areas full of trafficked staff; they often operate from prominent city centre business buildings that can accommodate their often sizable workforce (hence the popular name 'offices'). They can be densely clustered – one pre-trial investigation listed six alleged scam call centres within a kilometre of each other in the Solomianskyi district of Kyiv.[52]

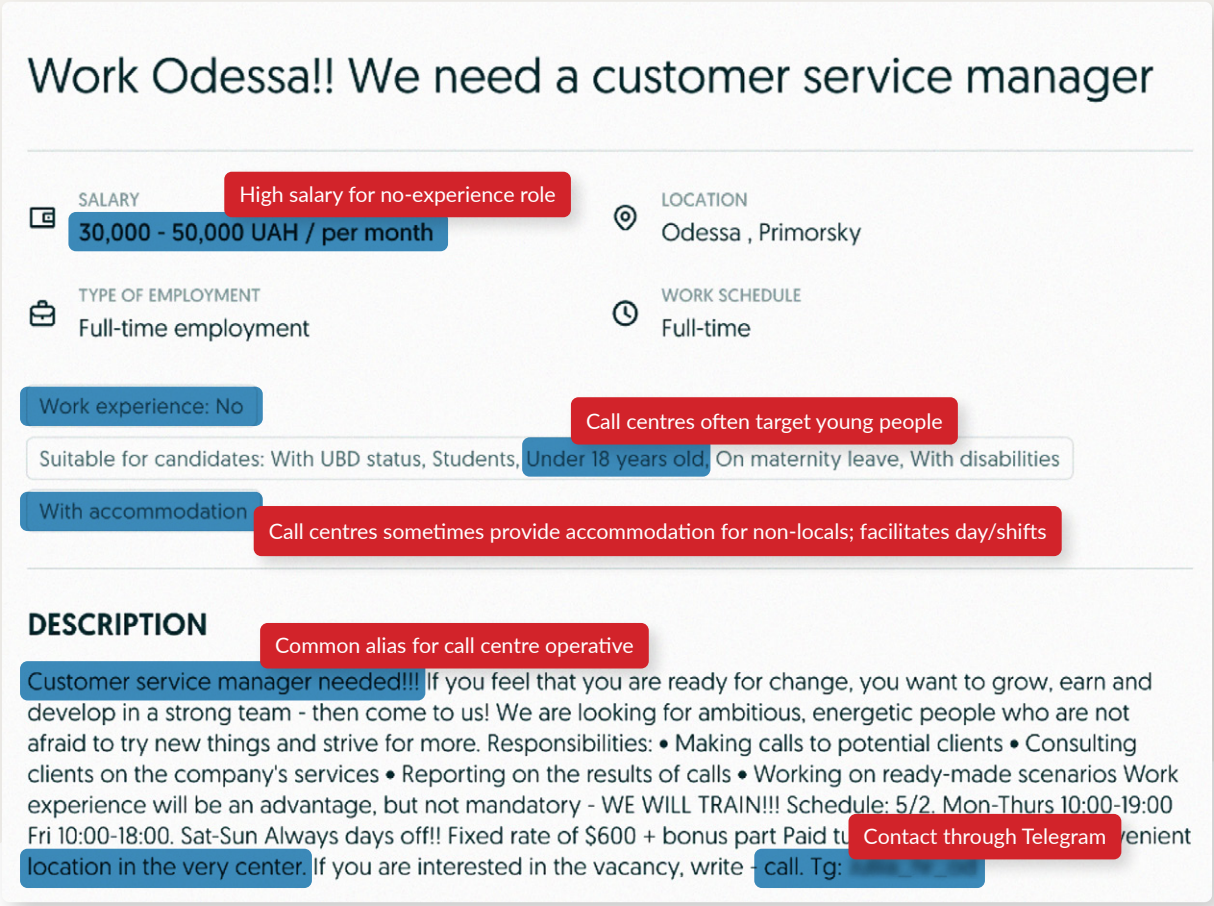
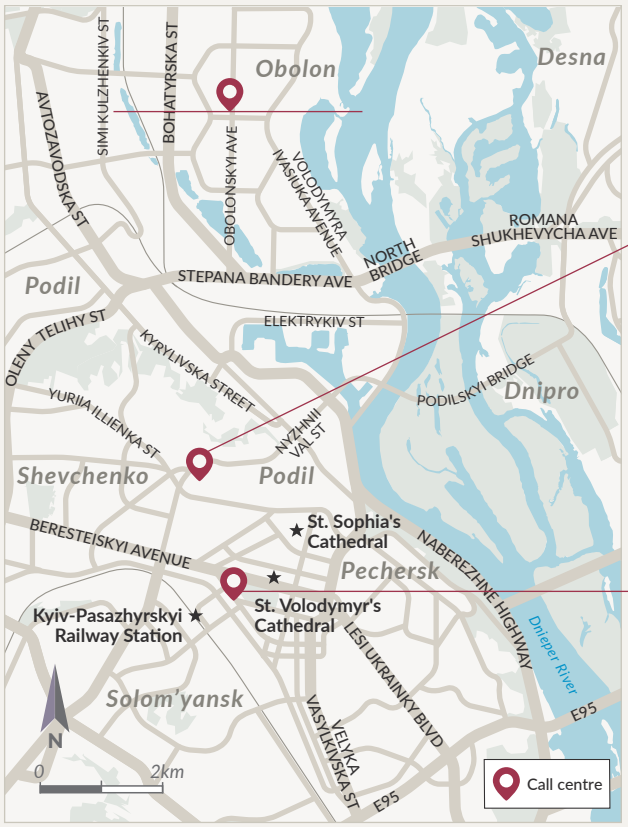


FIGURE 1 The highlighted information points to a role in a scam call centre.

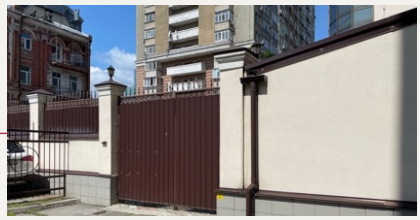
SOURCE: OLX (advert since delisted), https://www.olx.ua/uk/obyavlenie/rabota/rabota-odessa-trebuetsya-menedzher-po-rabote-s-klientami-IDXVY6z.html

But just because they are not hidden does not mean discretion is absent or security lax. Call centres often have security cameras, gates, keycards and human guards. Polygraphs are used to detect law enforcement moles, journalists looking for a story or other unwanted characters.

The level of discretion appears to vary according to the character of the city. According to a former call centre employee, 'In Kyiv you can't talk openly about "offices" in public. In Dnipro, everyone does [because] Dnipro has always been a more criminal city.'[53] One source claimed that Transcarpathia was too small for call centres to become a mass phenomenon, because they are difficult to hide.[54] But there were many reports of scam call centres operating,[55] especially in Uzhhorod and Chop – Uzhhorod perhaps because it is a fairly large city with more room to hide, while Chop is close to the borders with Slovakia and Hungary and away from the spotlight.[56]



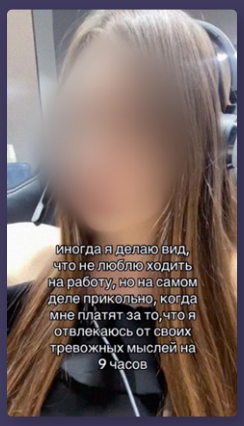
Scam call centres have been shut down at the Forum business centre, but some may continue to work there.
SOURCE: Interview with law enforcement, Kyiv, May 2025.



Tight security outside the Botanik business centre, where scam call centres have been shut down.
SOURCE: Interview with law enforcement, Kyiv, May 2025.

FIGURE 2 Locations of call centres in Kyiv.
SOURCE: Base map from Google Maps; photos supplied by the GI-TOC

Geolocating a call centre



To demonstrate the extent to which call centres operate in the open – and are therefore theoretically detectable by law enforcement – the GI-TOC set out to geolocate a call centre in Kyiv using TikTok. In its videos, this call centre repeated many of the common tropes associated with scam call centres.

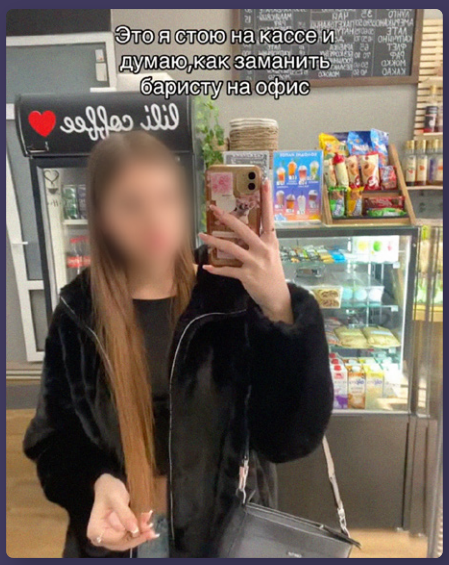
Stage 1: Finding the person

HR manager for call centres[57]

Stage 2: Narrowing the location

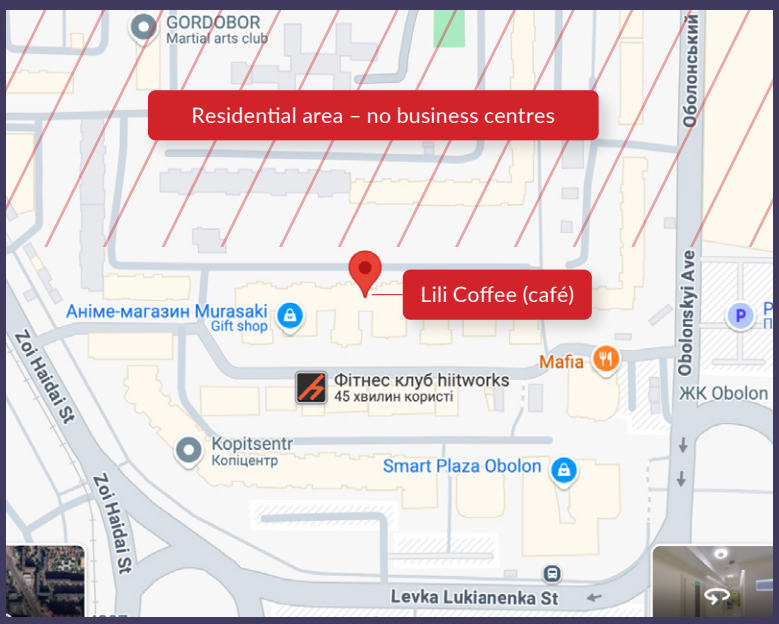
Two videos provide clues to the rough location of the call centre where the HR manager works. The first shows a woman bringing snacks to the office; behind her is a red Toyota registered in the Obolon district of northern Kyiv.

The second shows the HR manager in a coffee shop, with the caption, 'This is me standing at the cash register and thinking about how to lure the barista to the office.' Searching for 'Lili Coffee' (the name on the refrigerator) brings a result for a cafe in Obolon district. The typography of 'Lili Coffee' on the cafe's exterior sign matches the refrigerator. Assuming the HR manager was buying coffee on her way to work or in her lunch break, we narrowed the search to a 10-minute radius of the cafe.

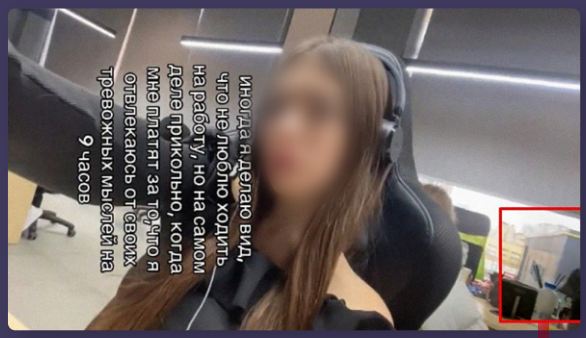


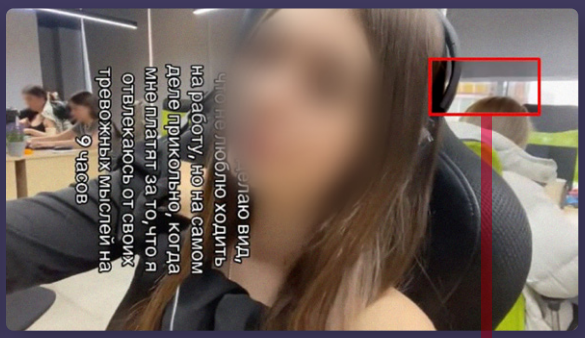
Stage 3: Identifying the building

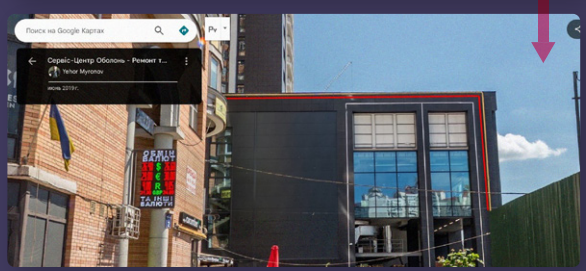
Half of the search area has no large business centres (as indicated by the style of the HR manager's office). In the other half there are several options, but another video offers a further clue: a building with a yellow stripe in the background. Later in the video we see another building with a yellow covering.

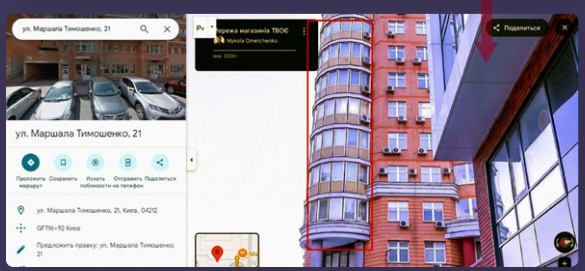


The building with the yellow stripe is Silpo supermarket in the Smart Plaza Obolon shopping mall (19 Obolonskyi Avenue). The residential building with the yellow covering on the balconies is nearby. This places the call centre at 21/14 Levka Lukyanenka Street.



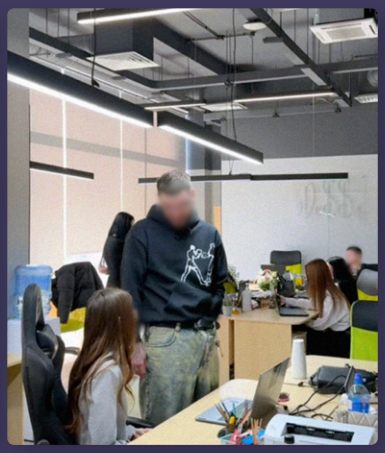


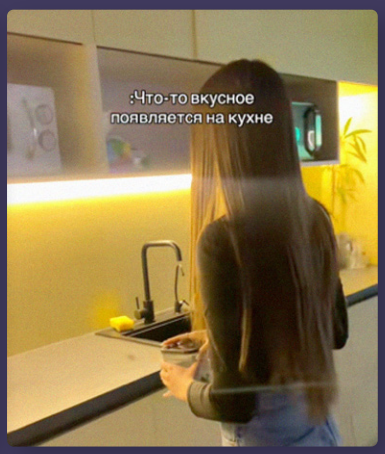




Stage 4: Finding the office address

Once the building was identified, we searched office space adverts and found a listing matching the setting shown in the call centre TikTok accounts, which was posting between July 2024 and April 2025.[58] See, for instance, the chairs and the distinctive lighting and style of the kitchen. Based on the estate agent's listing, the office is on the third floor of a business centre, with space for 58–65 desks. The office was advertised for rent in July for US$12 000 a month, indicating that the call centre had moved or closed.[59]





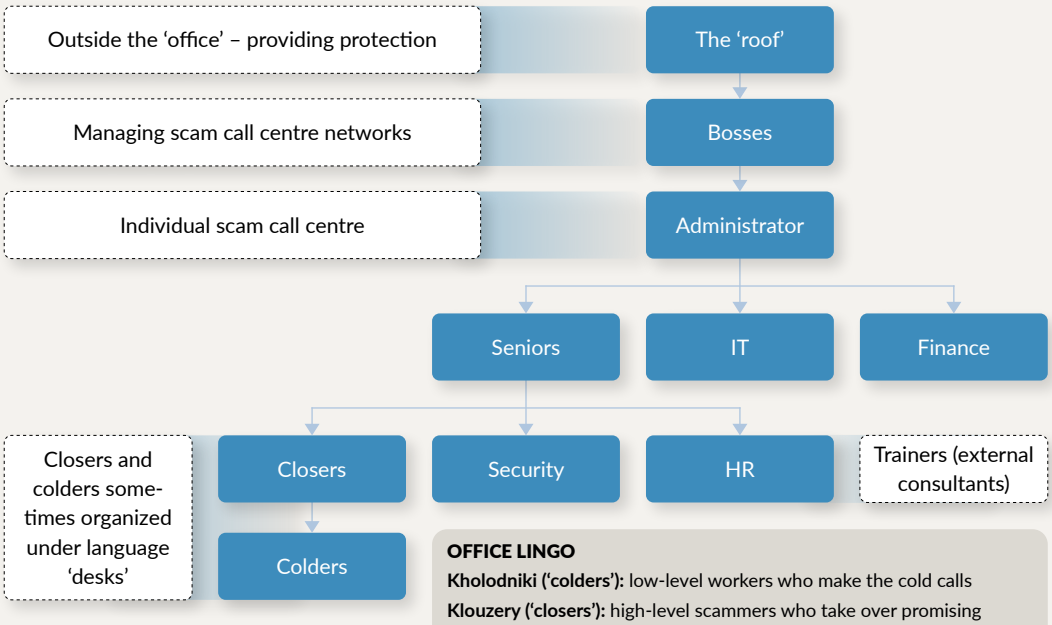
Highly networked, criminally connected

Call centres operate with strict hierarchies. At the bottom are the *kholodniki* ('colders') who cold-call potential victims. Above them are the closers who lead victims through financial transactions; staff in this tier are not necessarily in the same office as the *kholodniki* but are in constant contact with them online. The HR team handles personnel, including recruitment. The IT team handles software, technical support and IP telephony, among other tasks. It is at the core of the organization's technical capabilities, which can include sophisticated tools for faking websites, apps and documentation. The security department handles access to the office and internal discipline.

At the top, administrators run the office.[60] An administrator handles accounting and the money flow, and liaises with the owners, who are rarely seen by other call centre employees. Such a closed and vertically integrated hierarchy guarantees that a low-level employee knows nothing consequential about the real money-makers.

Scam call centres constantly evolve and improve. Inexperienced *kholodniki* attend training courses on how to handle clients. Some 'offices' reportedly hire psychologists and other trainers to hone scammers' techniques, using recorded conversations for analysis.[61] Computer logs are constantly checked and mobile phones are left at the entrance to avoid potential leaks. Scripts must be memorized. There are motivational sessions and a system of bonuses to reward success. According to an EMA representative, the most advanced call centres continually learn by working on incident management, thoroughly analyzing failed cases, and then revising their procedures and scripts to avoid similar mistakes in the future.[62]

Owners often have stakes in many 'offices', sometimes covering several cities and regions, creating a network or 'grid'. According to one former employee, 'All call centres belong to several groups. There aren't that many owners – it's like a mycelium.'[63] In part, this is because the call centre is an eminently scalable form of criminal enterprise, requiring only a few protocols or scripts, office space and technology. Once an 'office script' has been created it can be used repeatedly. A former employee described a building with 100 people working in four offices 'which were friendly because they belonged to the same group'.[64] Other networks are more regionally dispersed, such as one exposed in December 2023 with call centres in 16 oblasts and a reported 2 500 staff.[65] Many networks also have an international dimension.



OFFICE LINGO
Kholodniki ('colders'): low-level workers who make the cold calls
Klouzery ('closers'): high-level scammers who take over promising 'clients' and defraud them
Ofisniki: general term for a scam call centre worker
Temshchiki ('themers', 'scammers'): call centre worker
Mammoths: 'targets' to scam
Vyshka (the 'tower'): the investors, owners or top brass, the bosses of a call centre
Grid: a call centre network comprising multiple call centres under a single overarching hierarchy

FIGURE 3 Simplified organizational diagram of a scam call centre.

Two of Ukraine's three biggest 'grids' are reportedly run by 'traditional' organized crime players, the Dnipro networks and Khimprom.[66] The Dnipro networks have a long history of involvement in illicit activity. Forged in the 1990s, these criminal groups became some of the most powerful in Ukraine, operating in traditional illicit markets such as drugs and extortion before they 'started thinking and came up with something new'.[67] Lasha Svan, a Dnipro 'thief-in-law' (the term used to describe an established member of the post-Soviet underworld), for example, is closely linked to scam call centres.[68] He is a partner of another thief-in-law, Serhiy 'Umka' Oliynyk, who is associated with the influential Dnipro businessman Oleksandr 'Narik' Petrovsky.[69]

Saksahanskoho Street in Kyiv, where a police document says a scam call centre operated on the eighth floor. It was notable for having indirect ties to a prominent Dnipro underworld figure and for being staffed by Turks, indicating a new scamming target. *Photo supplied*

According to a former employee, one of the most notorious Dnipro groups is the Nines (Devyatky), which she described as the 'most brutal – they can take you to the forest … They have the most terrible offices, they still exist, they still work. If you want to join another gang [you always know if you're working for the Nines] there can be big problems. If you leave the Nines you will never be able to work in an "office" again – you make a promise.'[70] The Nines reportedly ran the biggest scam call centre in Dnipro until it was raided in 2024.[71]

The other major grid is reportedly run by Khimprom, a drug trafficking organization that specializes in synthetic drugs. It emerged in 2014 on the dark web in Russia and has since expanded to Ukraine and beyond.[72] Khimprom initially developed call centres for the drug market, suggesting that fraud may have been a retooling of existing infrastructure and personnel.[73] In addition to Ukraine, the Russian state media agency TASS reported that the Khimprom leader also manages call centres in Russia and, according to the MP, Europe and Asia.[74]

Officially protected

Taking down scam call centres is difficult. No dedicated legislation tackles this type of cyber-enabled fraud, which currently falls under Article 190 of the Ukraine criminal code, which applies to fraud in general. Law enforcement also require victim testimonies before launching a case, and many victims may be too embarrassed or ashamed at being scammed to make a formal complaint. Tracing the location and mapping the activity of a scam call centre is also complex work that increasingly demands high-level technical skills and resources. The cell-like structure of call centres, in which the bosses are largely insulated from day-to-day activities, also means individual operations rarely damage the coordinating system.

But there is one more aspect that makes legal interdiction much harder and in some cases futile: protection. Call centres, like several other forms of organized crime in Ukraine, have long benefited from *krysha*, or a 'roof' – in other words, a form of protection from law enforcement agencies.[75] In exchange for a fee, scam call centres are allowed to work; if a raid becomes necessary, the call centre may be given advance warning, or it may be raided on the tacit understanding that operations can resume after a show of performative justice.

There are nuances in the sphere of protection. A former employee said she had worked at a 'grey' call centre – one that did not have official protection but 'followed the rules' by targeting only Russia.[76] These 'rules' were semi-codified: the MP who worked on the call centre commission described how 'we had a non-public agreement with two law enforcement agencies that "their" call centres would be regulated by internal documents … to guarantee that they would be working against Russia and not Ukraine or other countries which were not Ukraine's enemies. Both of them are serious about this. [If you break the rules], the fact that "your" call centre is working against Ukraine's friends will come out and hit you.'[77]

A 'black' call centre, by contrast, has a 'roof' and does not care who it targets.[78] These call centres pay for their protection, often from the police and prosecutors. Raids are largely for show: three former employees of different call centres reported witnessing police raids that ended as soon as the corrupt officers received their money.[79] '[The police] shut the call centre down, kicked everyone out. The employees got a day off – the next day everything went back to business,' said one former employee.[80] 'The "roof" is the police,' said another. 'It's all about personal connections.'[81]

The involvement of law enforcement in these arrangements was confirmed by the MP, who said: 'Law enforcement provides a roof. Whenever the commission went to work in a certain region, local call centres stopped their activities for two or three days. Law enforcement agencies were warned about the commission coming over and the places it would visit. So, it's obvious where the leaks came from.'[82] Another commission member said this aspect of protection was one of the reasons the commission was established in 2023: '[The issue] is no longer about the formation of a new type of criminal business, but about the formation of a criminal elite that fits into the structure of interaction with law enforcement agencies and local authorities.'[83]

The cost of providing a roof varies, though two figures cited were between US$10 000 and US$15 000 a month.[84] According to the MP, 'The call centres have a special person to deal with these issues. This person approaches a law enforcement agency and tells them the call centre is willing to pay a monthly fee for a roof. Usually, a deal is struck with just one law enforcement agency, but [it] needs to provide protection from other agencies. The agency receives its fee and shares it with other agencies, asking them not to interfere.'[85]

A residential building in Kyiv where a scam scall centre was investigated. In July 2025, it still appeared to be operational, with good security and large numbers of young people entering at lunchtime. *Photo supplied*

Global reach

For reasons of language and politics, scam call centres in Ukraine began by targeting Russians and Ukrainians, but today their victims are drawn from a global pool. Even before the full-scale invasion, the Milton Group, for example, demonstrated an international reach.[86] Others have morphed from 'patriotic' scamming to more comprehensive operations. A former employee said when she began working at a call centre she targeted only Russia, but went on to work in Ukraine and elsewhere in Europe.[87]

To access the greater riches of EU countries, language teachers are sometimes employed.[88] Many call centres have language 'desks' that handle different markets, with English-language markets the most profitable. Prominent target countries include Czechia, Latvia, Poland, Romania, Canada and the US, but the extent is vast.[89] Scam call centres with ties to Ukraine may also be migrating further afield, with cases reported in Poland, Bulgaria and Greece, among others.[90]

As well as the potentially larger rewards for scamming 'rich' Western countries, going global also obeys one of the primary rules of scamming: don't work in your country or against it.[91] This is less for ethical reasons than because it is more difficult for foreign countries to trace a scam and launch an international investigation than it is for domestic agencies to pursue cases in their own back yard. Distance, in other words, confers a form of immunity. The complexity of scam call centre investigations means that transnational cases that are brought may take years to work through the court process, and some arrests may not translate into convictions (see box below).[92]

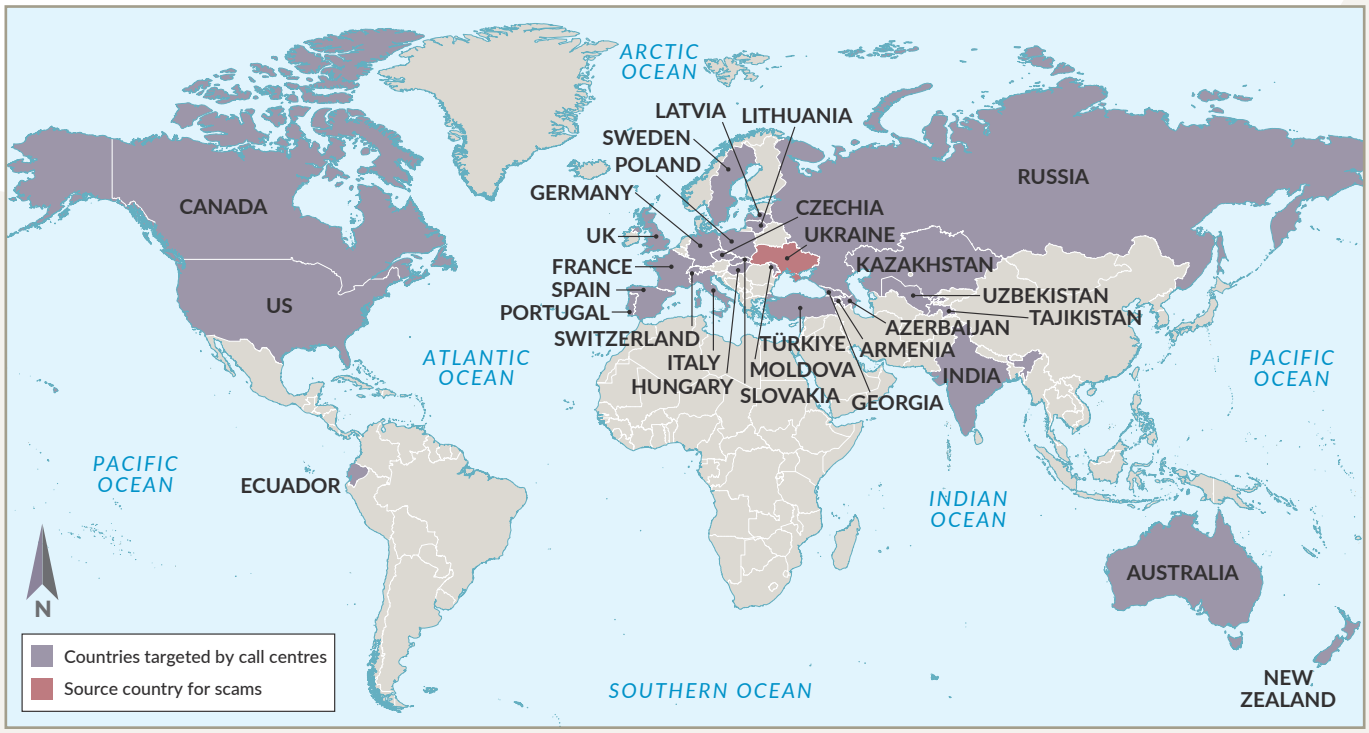
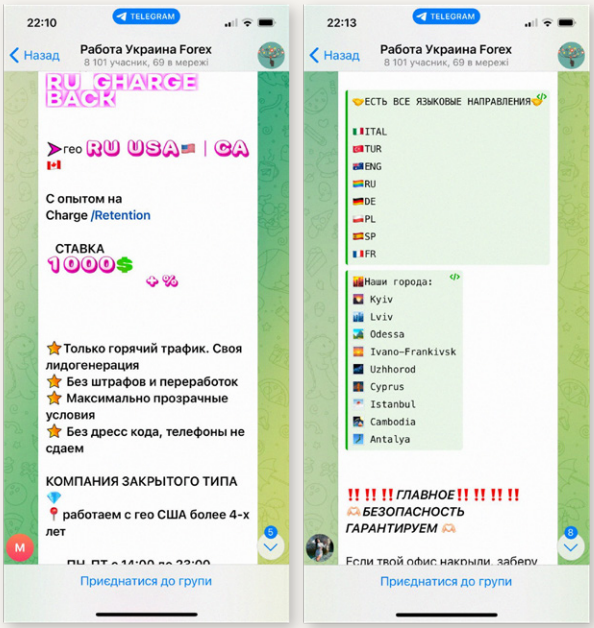


FIGURE 4 Countries targeted by Ukrainian call centres are largely in the Global North, where the potential to scam more money is higher.

SOURCE: GI-TOC research



A call centre recruitment advert on Telegram highlights desired language skills and target countries, including Turkey, Cyprus and Cambodia.
Photo: Screengrab from Telegram

How a transnational scam investigation fizzles out

Arrests against scam call centres targeting foreign citizens may make headlines, but the success of the subsequent prosecution is sometimes another story. A call centre in Khmelnytskyi, for example, was shut down in June 2023 after running a scam that tricked Canadian citizens. Masquerading as a defunct UK-registered company called Blockchain, it promised to transfer money made from trading on blockchain exchanges.[93] To secure the funds, the scammers persuaded the victims to install the AnyDesk programme, which allowed them to gain remote access to victims' accounts.[94] According to official comments from a representative of the Khmelnytskyi regional police, the scammers defrauded representatives of the Ukrainian diaspora in Canada and Canadians who helped the Armed Forces of Ukraine.[95]

The scammers' total reported takings were relatively small – less than US$5 000 from six victims[96] – but the perpetrators still faced lengthy prison terms. However, the case soon stalled, according to the open part of the court register. After several actions, such as the granting of bail and the extension of the pre-trial investigation period,[97] the case seemingly went cold in November 2023 when one suspect's bail was returned and he was placed under reduced oversight measures (such as not leaving the city or communicating with witnesses). The seizure of several iPhones and laptops was also cancelled in November 2023, presumably indicating that these were returned to the suspect.[98] There was no information that the term of the pre-trial investigation was extended again, or that the pre-trial investigation had been completed and the indictments sent to court.

The last update connected to the case came in September 2024 when the State Bureau of Investigation (DBR) launched a pre-trial investigation into Khmelnytskyi regional police officers involved in the Canada case. There were concerns that they had abused their official position and appropriated a small amount of money (UAH200; equivalent to about US$5) and several iPhones connected to the case.[99] Without further information, it is impossible to ascertain the status of the case or the reasons it has stalled, but it illustrates that headlines about arrests do not always translate into prison sentences. ■

Tech-enabled

Telecoms is at the heart of call centre fraud but today the illicit industry can call upon the much broader suite of technology used in modern information architecture, from website and app development to marketing algorithms on social media.

At every stage, technology helps boost the scope, scale and secrecy of scam call centres. Recruitment is done in part online through job websites and social media. Deepfakes and voice-cloning technology can convince victims they are receiving advice from a trusted source or communicating with a friend or family member. AI-enabled translation removes the language barrier between scammer and target, and AI can help fool verification processes. AnyDesk, TeamViewer or even accessibility apps for people with visual impairments (misused for remote access) are employed to take control of victims' computers. Within seconds, automated design tools embedded in fraudulent admin panels can generate realistic images of bank letters, completed with the victim's account information and corresponding documentation with stamps and signatures.[100] Scammers persuade victims to download 'new' banking applications, giving them access to financial information, or persuade them to transfer their number to a different SIM card, with the same result.[101] Even Diia, the state's official app used for a variety of services, has a convincing fake doppelganger.[102]

At the heart of social engineering is knowing your customer, and one of the most powerful tools for call centres until it was taken down by the Russian authorities in March 2025 was God's Eye, a Telegram bot. It helped to analyze big data across a range of platforms, from social media to search engines and websites, to construct a detailed map of relationships between indicated points of interest. Such data could include personal information, including card details and passwords, which helped scammers build detailed profiles about their potential victims, increasing their 'trust leverage' when it was time to call.[103]

Other scammers use the dark web to buy databases of potential victims, including those with a propensity for online gambling, taking loans and playing on the stock market.[104] VoIP is often used in spoofing – modifying the caller ID number shown on the victim's screen – to mask scammers' origins.[105]

In-office security is also high. VeraCrypt, open-source disk encryption software, is used to protect workplace hard drives, passwords are 20–30 characters, and customer relationship management software can be accessed only from certain IP addresses ('IP whitelists') – the same approach used by IT administrators to protect their infrastructure from scammers.[106]

Technology is also critical to the handling of money, from the use of 'drops' (bank accounts of third parties used to receive, move and cash out money) to cryptocurrency wallets, exchanges and mixers (which mix potentially identifiable or tainted funds with others to obscure the trail back to their source).

LIFE INSIDE A CALL CENTRE

The GI-TOC's interviews with former employees of scam call centres reveal a world that is often a far cry from the one advertised. Instead of high salaries and a start-up style workplace, recruits often find themselves working long hours for little pay and are often subject to coercive behaviour and micromanagement.[107] For the most part, getting a job is easy – it is leaving that is problematic, especially for successful scammers, with threats, violence and blackmail used to 'persuade' them to stay. While not on a par with the human trafficking seen in South East Asian call centres,[108] those involved in scamming in Ukraine may occasionally be victims of crime as well as its perpetrators.

Getting in

Call centres hire a broad range of people. In general, those between 15 and 28 years old are preferred (although 'grandmothers can be very convincing', said one former employee).[109] At an information-sharing session of the call centre commission, activists claimed that 'the vast majority of call centre "employees" are aged from 14 to 20'.[110]

HR managers are responsible for attracting new recruits. 'You can easily recognize an office HR,' said a former employee. 'A glamorous lady in her 20s … pretty, nice voice, acts as bait.'[111] HR departments also use 'success stories' – high-flying 'colders' who try to recruit their friends or impressionable strangers.[112] A former employee recalled being approached at the age of 15 by older boys who showed him their money and said he could make some too. The next day, the older boys picked up five younger ones and took them to the call centre for training.[113]

Some new recruits are aware of the true nature of the work they are signing up for, but others may attend an interview after being given false information. One employee was told she would be selling generators but learned at the call centre that she would be trading cryptocurrencies. It was only when she accessed the system and found out she would be using Badoo, a dating app, that she realized it was a scam and left. (A few days later, she was asked to join the HR department, where she tried to find recruits on the websites work.ua and robota.ua using the same 'cryptocurrency trading' story.)[114] A 16-year-old boy was contacted about a job delivering leaflets, only to find out at the interview that the job did not exist. But another job did – calling people in different countries.[115] The HR team told him 'we have money, a warm office' and he could make big money. 'There's this boy working at the office, he's 16,' they said, 'and he has already bought his mother a car, a phone, a computer.'[116] He declined the offer and left.

The job

Most call centre employees are lured by offers of good working conditions and high pay, especially for teenagers or those finding their first job after university, but the reality often disappoints. One recounted being offered US$800–US$1 000 but was paid only US$200 and told the rest had to come from commissions on sales. In the end, she made only UAH10 000 (about US$250).[117] Another was promised a daily rate of UAH1 500–UAH2 000 but earned only UAH300.[118]

While it is possible to earn big money – the GI-TOC was told of scam callers earning up to UAH100 000 (US$2 400) in a day, and one who earned UAH300 000 (US$7 250) in a week[119] – a former employee said 'getting rich at a call centre is random, it's all a matter of luck. There is no "success story".'[120] The system makes it difficult to reach the promised levels, with commission being staggered depending on the number of clients who are 'closed'. Those who close only a few clients will earn little commission.[121] One call centre had a system of fines for offences such as mispronunciation, being late and taking long coffee breaks.[122] This mirrors the practice in the legal call centre sphere.[123]

The pace of work is intense and targets are high. One small office of 25–30 people, for example, had a minimum target of half a million rubles (US$6 400) a day when scamming Russians. An employee recounted calling 200–300 people a day, with a third engaging in conversation. Of this number, seven might be 'closed'.[124] According to an EMA representative, some scam centres make up to 5 000 calls a day. Only about 0.1 per cent of targets remain on the line for more than 10 minutes — a strong indicator that these victims were likely successfully defrauded.[125]

Scammers can work for 12 hours a day, six or seven days a week if they are not meeting their targets, and they are under constant pressure and surveillance. 'The work is hard, you have to sweat and try to "close" as many people as you can … You lie all the time,' said a former worker.[126] To maximize profits, some offices run day and night shifts targeting different time zones. Some provide housing to employees who are not local so they can be available to work either shift.[127]

Getting out

Those who do not hit their targets may be fired, but those who do – especially closers – find leaving a call centre much more difficult. 'If you make them a lot of money they set the bar higher,' said the former HR manager. 'They will find ways of making you stay.'[128]

Those who try to leave might be subjected to threats and physical violence.[129] 'They usually let the colders go easily,' said the former HR manager. '[But] if the good ones leave without permission, they may be found and punished. They beat them with wire until they bled, and people were shown a photo.'[130] A former employee said he had heard 'about what they can do to your fingers, hands and feet. If you try to get away, they can take you to the forest.'[131]

This especially applies to employees moving to a rival call centre network, or 'grid', although moving within a grid is acceptable. As the former HR manager said, 'There's always several offices in one building – it's all one grid. You don't work for other grids – that has consequences.'[132]

Even for those who escape call centres, there is a price to be paid. Working in such places, interviewees agreed, changes a person. One former employee spoke of the 'callousness, greed, an emptiness in the eyes' of scammers.[133] 'Your attitude towards yourself definitely changes,' said the former HR manager. 'You think if you've robbed someone else, you've won. In your own eyes, you're a winner.'[134] Lying becomes second nature.

But this is by no means universal. The HR manager said her experience was 'hard morally and psychologically. It's degradation, you hear negative things on the phone all day. I felt sorry for those people [the victims].' Nowhere was this internal conflict starker than when scamming Russians. On one hand, the HR manager approved of this in general, 'but 500 000 [rubles] from a grandmother [saving for her funeral] because her children don't talk to her any more? That's different. You think that you are a ruler, you use moral violence, [but] you're just a crook.'[135] She concluded: 'Call centres are a trauma for everyone who works there.'[136]

The real trauma of call centres, however, is suffered by victims. Most scammers are either not affected by such qualms, or not to the extent that they overcome self-interest, and judging from the data leak that led to the OCCRP investigation, many relish defrauding victims.

For the victims, financial losses are often substantial. They can lose their life savings, their homes and the money of others, often borrowed under false pretences. Heavy loans may also be taken out in the victim's names without them knowing. But the damage can run far deeper, including feelings of shame, embarrassment and a damaged sense of trust. And the sophistication of call centres means money will seldom be returned and perpetrators hardly ever brought to justice. Worse, having been scammed once, the chances are higher that they will be scammed again, as scammers target those who have fallen for such deceptions in the past. According to the EMA representative, 'Statistics show that those who have become victims of fraud fall victim again and again.'[137]

FUTURE TRENDS: DECLINE OR ADAPTATION?

Have scam call centres in Ukraine already hit their peak? Some analysts believe so, detecting a fall from recent highs.[138] According to the EMA, scam call centres were among the top five criminal threats in Ukraine in 2022 but dropped out of the top five in 2023.[139] 'The number of complaints [from Ukrainians claiming to have been scammed using the bank impersonation scam] is decreasing more and more,' said an EMA representative.[140]

If true, there are many possible explanations, from market fatigue to law enforcement action. Rising exposure to and awareness of call centres has made Ukrainians harder targets. 'People are already more or less aware of this topic,' said the EMA representative. 'When it comes to phone fraud of the type "your card has been blocked by the bank, please provide your card details for verification", there are now far fewer cases. People are aware of these simple schemes because media, banks and the National Bank have been running awareness campaigns. Moreover, many Ukrainian citizens, or their relatives, have already received such calls in the past.'[141] The MP on the commission agreed: 'The good thing is that people are getting smarter and don't get duped as easily.'[142]

The crackdown in 2023 also reduced the number of call centres, pointing to the fact that 'the business has become more expensive: law enforcement agencies can't help them so much for the same fee'.[143] Another opinion traced the drop in the number of call centres to the fact that so many young people had left the country.[144] The appointment of Ruslan Kravchenko as the new prosecutor general in June 2025 appeared to give new impetus to the fight against call centres, as seen in the wave of crackdowns in Dnipro and Kyiv the following month.[145]

Technology has helped shut off some of the traditional means of working. The pilot provision of internet services in pre-trial detention centres (which sometimes host scammers) was halted in October 2023, and authorities moved to block fraud calls and identify perpetrators calling from such places.[146] Russia passed legislation in December 2024 (to come into effect in September 2025) preventing IP telephony being used for scamming, principally by stopping VoIP being used with number substitution to make a victim think they are being called from within Russia (smurfing).[147] The new legislation will not prevent calls through social media applications but Russia has also made indirect noises about cracking down on Telegram, a major hub for scam activity. In launching the new 'national messenger' application, a Russian official said that 'many people ask me whether [it] means Telegram will soon be

blocked. I think that if [Telegram] strives to comply with the laws of the country in which it operates so actively, it will not come to such extreme measures.'[148]

But does this mean scam call centres are falling by the wayside? The evidence suggests not. What appears to be happening is the evolution of the old business model into something new, with increasing diversity, automation and sophistication.

Doubling down on the global market

Anecdotally, there may be fewer call centre adverts on online job sites and Telegram, but there is still plenty of evidence that call centres feel empowered to recruit on public channels.[149] Many of these adverts make clear that the global market is the priority. A sweep of robota.ua and olx.ua in July 2025 revealed high-paid roles in Kyiv for people with knowledge of German, Italian, Czech and Slovak. Even more troublingly, there were adverts in Russian and Ukrainian for roles in Slovakia and Poland with free accommodation. This indicates that Ukrainian call centres are becoming more active in Europe, where they are presumably attempting to recruit – and target– refugees.[150] A former employee said she had heard about call centres also emerging in Germany.[151] One of the more expansive job adverts in Russian sought candidates with expertise in any of 12 languages, including Japanese, Chinese and Arabic, and offered to provide accommodation 'all over Europe'.[152]

From business centre to remote work?

These adverts also provide a window into the changes the office model may be undergoing. In Ukraine, the physical office is still a fixture of the business. Many roles mention a 'modern office' in central locations, with Dnipro still the epicentre of large call centres. Many business and shopping centres refuse to rent space to call centres, as they care about their reputation and fear losing other tenants, as well as potential legal repercussions, yet there are still those willing to do so, since scam centres can pay significant money.[153] In the first half of 2025 a spate of arrests in Kyiv targeted call centres in large, centrally located business centres, including the Canyon, Mikom Palace and Prestige (Figure 5).[154]

But there are also signs of greater discretion. According to the MP on the call centre commission, call centres 'are starting to hide more and optimize their operations', such as hiring out-of-town industrial or storage space and bussing workers there for their shifts.[155] Due to their isolated nature, it is easy to have enhanced security at such sites, including concrete fences and dogs.

And despite the open advertising, call centres have become more conscious about vetting new employees, perhaps due to numerous stories by undercover journalists masquerading as employees. At present, call centres conduct stringent screening of candidates, including checks of prior work history and in some cases the use of polygraph testing. Interviews are increasingly seldom held at workplaces or in public cafés, reflecting heightened security practices.[156]

The adverts also point to a more fundamental trend – the gradual decentralization and dispersion of the 'office'. According to a journalist in Odesa, citing a former call centre employee, the logistics of call centres have changed significantly in 2025. Most operators in Odesa now reportedly work from home using services such as Starlink, gathering at least once a week for training and 'meetings'.[157] Similar trends are mirrored in adverts for call centres, which offer remote work using AI tools.

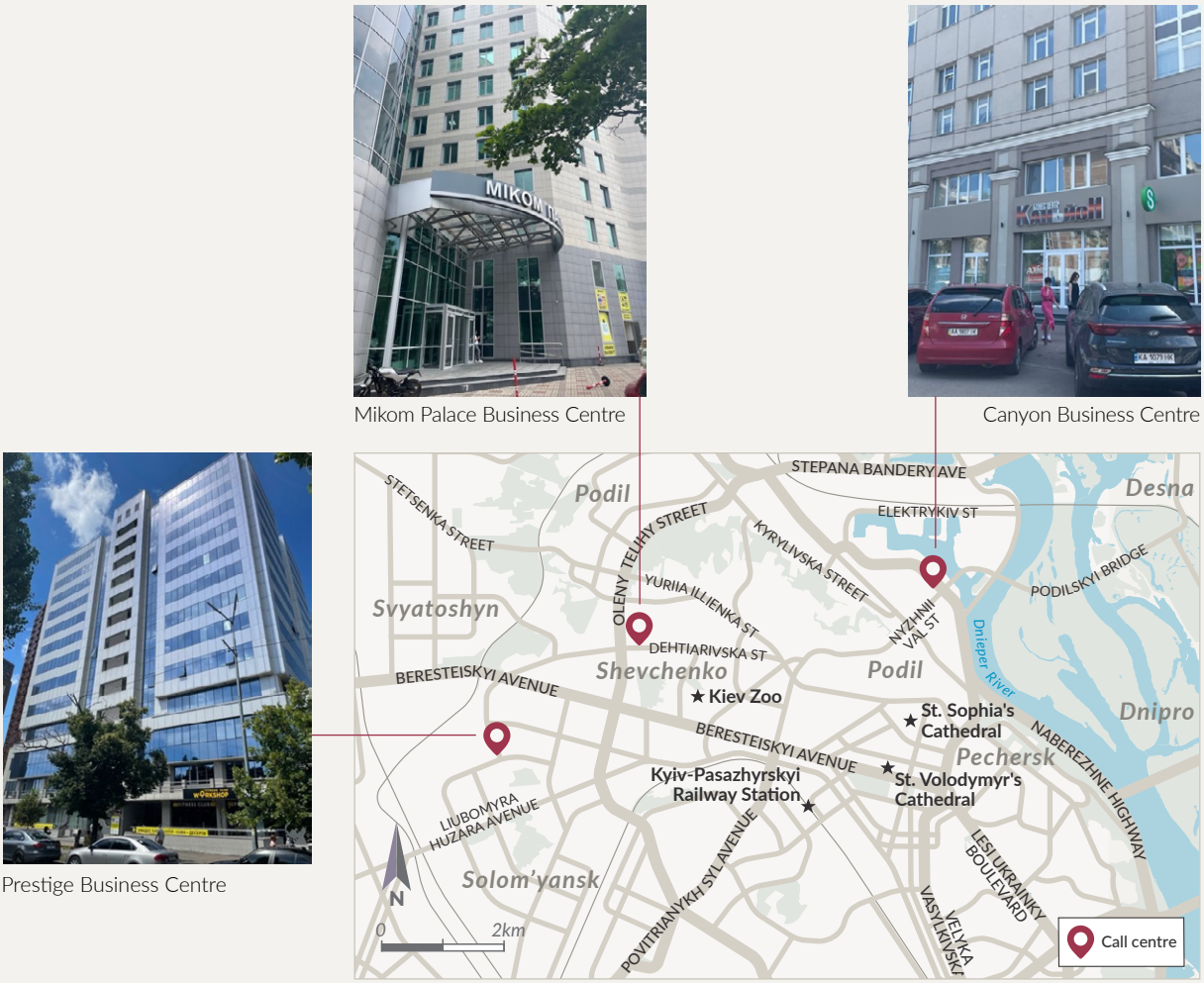


FIGURE 5 Alleged call centres were found to be operating in three large business centres in Kyiv in the first half of 2025.

While this shift may appear to reflect post-pandemic trends in the legal business sphere, it also points to larger changes that may fundamentally alter how call centres operate – and whether 'call' and 'centre' are even applicable any longer.

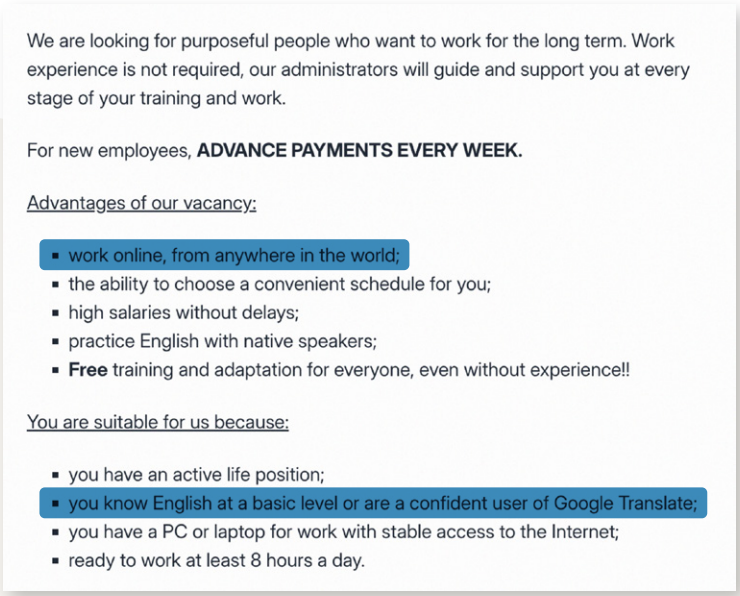
AI and crime as a service

In the future, AI and crime as a service may revolutionize scam call centres. Using AI, scammers can devise ever more ingenious methods to outfox security protocols and scale their activities to industrial levels by using software instead of employees. Social engineering can be conducted by bots instead of people, making the scammer more of an orchestrator than a player. AI has also overcome the language barrier, allowing for seamless translation in whatever language the scammer chooses.[158] According to Yurii Khmelenko, director of monitoring and countering fraud at Sense Bank: 'There is a decrease in the number of calls from scammers in favour of chat correspondence and the creation of schemes of maximum autonomy … They create advertising banners that motivate customers, target certain groups of people on social networks, encourage them to follow a phishing link, generate dialogues in which a person must specify their payment details or make a transfer without direct contact with the scammer.'[159]

Crime as a service is also game changing in terms of allowing new entrants to access the fraud market at scale and low cost. Today, providers offer 'start your own call centre' packages with operating scripts and manuals for how to hire employees – and sometimes with employees already identified. 'You choose

the brand, the country, the victims in those countries, the language which is yours or which you know very well. Even if you don't speak the language, you find a partner in the same programme who will make the call.'[160] Client databases, customer relationship management (CRM) programmes and money laundering services can all be bought off the shelf. An EMA representative reflected, 'a person does not have to sit in an "office" – he sits on this platform. And as such, there is no physical call centre.'[161]

As in the licit call centre world – also faced with the challenge of AI[162] – these advances may cause difficulties for the hierarchical, physically based and heavy headcount operations of scam call centres. If a scammer can perform all the same operations as a call centre from a bedroom with one computer, what need for the large office and official protection? And how will law enforcement respond when faced with numerous individuals instead of large, consolidated networks?



We are looking for purposeful people who want to work for the long term. Work experience is not required, our administrators will guide and support you at every stage of your training and work.

For new employees, **ADVANCE PAYMENTS EVERY WEEK.**

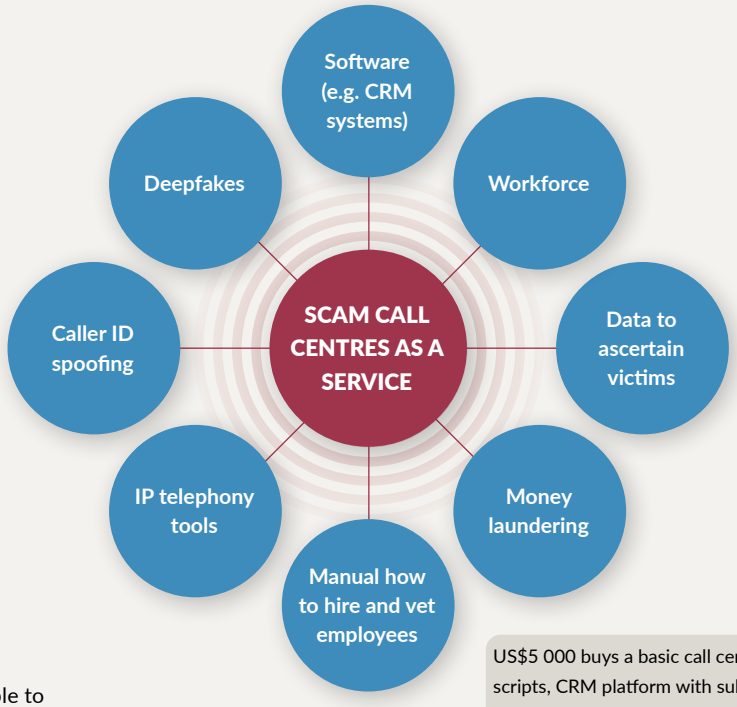
Advantages of our vacancy:

- work online, from anywhere in the world;
- the ability to choose a convenient schedule for you;
- high salaries without delays;
- practice English with native speakers;
- **Free** training and adaptation for everyone, even without experience!!

You are suitable for us because:

- you have an active life position;
- you know English at a basic level or are a confident user of Google Translate;
- you have a PC or laptop for work with stable access to the Internet;
- ready to work at least 8 hours a day.

A Ukrainian-language advert for scam call centre staff accessed in July 2025. The advert 'location' is in Prague, but the role is remote. *Photo: Jooble, https://ua.jooble.org/jdp/-6874012178798191861*



US$5 000 buys a basic call centre set-up: scripts, CRM platform with subscription and 10–15 employees. (Physical space not included.)

FIGURE 6 Services available to would-be call centre scammers.

RECOMMENDATIONS

Tackling the call centre ecosystem depends on addressing its five interlinked characteristics.

Close the shop window

Characteristic: Open but secure

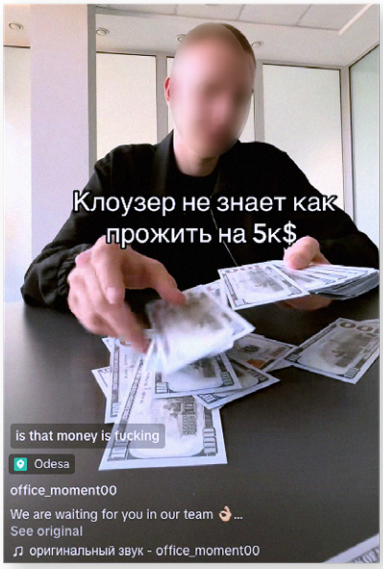
Recommendations

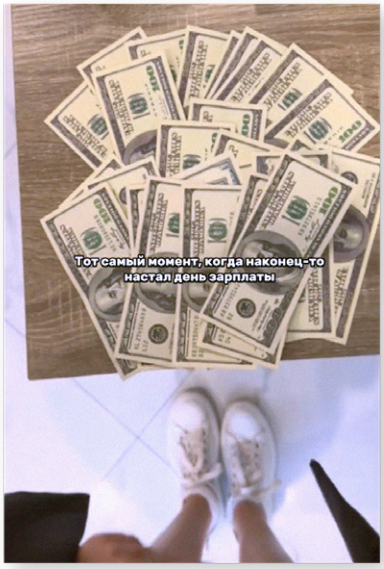
- Improve screening of job websites and social media, including sharing intelligence with law enforcement and new legislation.
- Raise public awareness of the gap between promise and reality at scam call centres when it comes to pay and working conditions.
- Incentivize landlords to stop scammers renting office space.

Scam call centres in Ukraine advertise and operate largely in plain sight. Disrupting these open working methods will make it harder to attract a steady stream of employees, which is critical to the high-turnover call centre economy. Some job sites are already being more careful about suspicious offerings, but such adverts are often carefully crafted to appear legitimate, and websites often have limited security budgets and expertise to screen the flood of offers from scammers. Cooperation with law enforcement could help address this problem indirectly. Once word gets out that job sites are being used for law enforcement intelligence gathering, call centres may be disinclined to keep using them. A similar approach could also work for social media platforms.

A fundamental attraction of call centres is their reputed high salaries, which are having a warping effect on the economy. Discussing two Ukrainian cities, an EMA representative said: 'Sometimes it's impossible to find a sales manager or find an employee for a normal call centre, because salaries in scam centres are much higher.'[163] But as this report has argued, the gap between promise and reality is often vast, with many employees receiving only a fraction of the large salaries mentioned in adverts. And the difficulty of leaving these 'dream jobs' is also a little-known aspect of working in call centres. Raising public awareness of the 'scamming of scammers' through the same channels used to recruit young people (robota.ua, work.ua, social media) may help dispel the 'get rich quick' aura surrounding scam call centres.

Blocking would-be scammers from renting prime city centre business space is another tactic. A stick and carrot approach may work best: landlords could be incentivized to support worthy legal businesses (such as those employing or run by military veterans) through tax credits or other such means, and sanctioned if they are found to have failed in their due diligence when leasing space to scammers.





Adverts for work in scam call centres on TikTok frequently emphasize the money that can be made. Dispelling this myth may make it harder for such centres to recruit. *Photos: Screengrabs from TikTok*

Legislation has a key role to play. As a member of the commission said, 'there are large loopholes in the legislation that allow you to freely recruit personnel for call centres, freely advertise them on social networks, rent premises, gain access to servers, [conduct] various financial transactions'.[164] Updating legislation to address the 'shop window' and physical infrastructure of call centres will bring gains on the ground.

The risk of this approach is that it may accelerate the trend of call centres moving out of cities or online, but reclaiming city centres and business hubs for non-criminal activity should be a priority. New methods will be needed to tackle the second-order effects.

Take down networks, not call centres

Characteristic: Highly networked, criminally connected

Recommendations

- Ensure fraud cases end up on the correct law enforcement desk.
- Build cases against networks, not individual call centres.
- Revisit the legislative recommendations made by the temporary investigative commission established by the Verkhovna Rada to introduce new articles to the criminal code on electronic communication fraud, with other applicable legislation.

The highly networked nature of scam call centres in Ukraine means there are relatively few big fish to target, and domestic cases are difficult to build for several reasons, not least official protection. However, looking at the issue from a law enforcement perspective, several operational bottlenecks and organizational issues could be addressed to help prosecute cases effectively and begin to erode these large networks from the ground up.

Most reports of fraud are usually made to the National Police and not online to the Cyber Police, and may get lost or end up on a desk where expertise, experience and capacity to tackle sophisticated call centre fraud are lacking. Even when the victims lodge a complaint in the correct office, a successful prosecution does not always result. According to an EMA representative, there have been cases where fraudsters approached their victims and paid them to withdraw their complaints, critically undermining prosecutions. This reduces the motivation of the Cyber Police to pursue such cases – although they

do continue to work on them. As the representative explained: ' [T]he main thing for our clients is to get their money back and the main thing for the Cyber Police is to put the bad guys in prison. These are different priorities.'[165]

Streamlining and safeguarding fraud complaints is therefore essential. Ukraine's many law enforcement agencies must know who is responsible for tackling fraud, and they require a mandate to compile individual cases into larger prosecutions against overarching networks. Shutting down individual call centres may look like progress, but the ease of restarting them makes this atomized approach akin to 'whack a mole'.

To give the law greater teeth, legislation must be updated to recognize the severity and reach of this form of crime. This was the path proposed by the temporary investigative commission established in 2023 by the Verkhovna Rada to investigate possible fraud by call centres. The commission proposed updating the criminal code by adding articles on 'electronic communication fraud' that would cover call centre activity, but parliament did not pursue the idea.[166] Reviewing this decision could provide law enforcement and prosecutors with more precise legal definitions, powers and sanctions to tackle call centre fraud, although it will not be easy. As the MP who worked on the commission reflected, 'I see serious opposition to passing the laws.'[167]

Break the shield of protection

Characteristic: Officially protected

Recommendations

- Revive political efforts to focus on call centres.
- Western partners must make it clear to Ukrainian counterparts that protection of call centres harming European citizens is unacceptable.

No responses will be truly effective while scam call centres continue to enjoy the protection of law enforcement. Breaking this shield of protection should be the primary goal of policymakers looking to move the dial on the call centre issue.

There are positive signs. There has been much media reporting in Ukraine since 2023 about the 'roof' offered by certain agencies, bringing the issue into the public domain, and there are signs that the risk calculus is changing. According to the MP, 'There's mounting pressure on law enforcement … [They] understand the risks connected to cooperating with scam centres.'[168] Ruslan Kravchenko, Ukraine's Prosecutor General since June 2025, has also led a renewed wave against scam call centres, with a string of high-level busts taking place in the second half of 2025 across the country, suggesting that the climate of impunity may be under serious strain, and perhaps fundamentally rupturing. Speaking in November 2025 after a joint operation with European forces, Kravchenko declared 'international cooperation works, and the border is no longer a tool to hide from justice'.[169]

But to definitively break protection, more is required domestically and from international partners. In Ukraine, it is critical to generate renewed political will to fight call centres. The temporary investigative commission was not renewed when its year-long mandate expired and parliament did not approve its report. One of the leading political figures involved in publicizing the fight against call centres, people's deputy Mykola Tyshchenko, reversed his stance in January 2025. After becoming embroiled in two scandals involving violence against military personnel, he said he had 'completely reconsidered his position' and would no longer oppose call centres.[170]

Western partners must continue to demand answers from international investigations into scam call centres that lead to Ukraine and go nowhere through Ukrainian courts. They must make clear that tolerance for forms of crime that harm Ukraine's Western partners is unacceptable, especially in the present circumstance of the war. As with all forms of corruption, the more light is shone on the issue, the harder it is to sustain the system.

Streamline international investigations

Characteristic: Global reach

Recommendations

- Developing streamlined international protocols to investigate international fraud will be the only way to keep pace with the exponential increase of fraud and lower the resource cost of transnational investigations.

Domestically, there are already strong tools to tackle scam call centres in Ukraine. Investigative journalism, for example, has played an outsized role in exposing the call centres' scale and reach. Financial institutions have also been at the forefront of the fight, with the Cyber Police recording a decrease in the number of scam calls thanks to cooperation with banks and financial regulators.[171] And increasingly these organizations work in tandem: there are successful coordination platforms between financial institutions, service providers, the Cyber Police and other government services.[172]

Building the transnational picture is more complicated. One of the major limitations in investigating the transnational workings of call centres is the reliance on large data leaks, such as the one that was used by OCCRP and other media partners to map out the Milton Group and AK Group (which in turn led to many tip-offs about the locations of call centres in affected countries).[173] Transnational takedowns must often depend on local law enforcement initiating investigations and seeking broader collaboration as the case dictates with the EU Agency for Law Enforcement Cooperation (Europol), INTERPOL or liaison officers, but local agencies often do not have large budgets to investigate the international dimension of fraud.[174]

Still, there has been much progress in recent years. Initiatives such as Europol's European Cybercrime Centre (EC3) and Joint Cybercrime Action Taskforce (J-CAT) are examples of approaches that pool resources and expertise on a multinational level within the EU, including with private sector partners. Both have previously worked with Ukrainian authorities to fight cybercriminals.[175] In 2023, the EC3 annual conference focused on the impact of the Russian invasion on cybercrime and cybersecurity incidents.[176] On the global scale, stakeholders are becoming ever more networked and conscious of the need to block scams in real time. The launch in October 2024 of the Global Signal Exchange – a joint initiative between Google, the Global Anti-Scam Alliance and DNS Research Federation – was a breakthrough in global information-sharing on scams.[177]

This sophisticated anti-scam architecture highlights the growing disparity between what can be done at the global, interconnected level and at the local level, where evidence is collected, collaboration sought and cases made. The missing piece of the puzzle, as is so often the case, is budget. For agencies faced with transnational scams, resources are especially hard to find if there is little prospect of recovering stolen funds, making arrests or if a successful prosecution is unlikely.[178]

The number of scams and their geography will only grow, so developing more streamlined and standardized international protocols to investigate transnational fraud may help lower the cost of

investigations and turn more cases into prosecutions. Even as the world gets better at tracing and tackling scams using technology, it must continue to ensure that national justice plays a key role in bringing global scam actors to book.

Maximize defensive AI with a political strategy and user responsibility

Characteristic: Tech-enabled

Recommendations

- Technology will be at the front line of responses to scams, but by itself it is not sufficient.
- Ukraine should develop a comprehensive anti-scam strategy that provides a coordinating approach for defensive AI, holds service providers to account and emphasizes the need for personal cybersecurity responsibility.

AI is transforming fraud, as it has in many other areas of life. Financial institutions are deploying 'defensive AI' against fraudsters, but the onslaught of scams risks undermining public trust in internet-enabled services.

As scammers find ever more ingenious ways to outfox verification systems, how can trust be maintained in the tools people use for everyday life? Tech can play an important role in combating fraud, but it may take more than banks reminding people not to disclose their sensitive information to help customers feel secure. Safeguarding citizens against fraud may require significant changes to the technological and legal landscape that only political actors can push through. A possible flagship example may be Russia, where the state's response to the surge in scam calls has a chance to be effective. According to the EMA representative, the Russian authorities are attempting to address the problem through restrictive measures — for instance, Roskomnadzor has blocked voice calls in Telegram and WhatsApp, and a single national messenger app is being developed. That said, these efforts – presented as part of efforts to combat fraud – may also serve to suppress freedom of speech (chats in the new national messenger are not end-to-end encrypted).[179]

But the fact remains that the state has a powerful role to play in creating a strategy that can reshape the response and challenge the narrative that scammers always have the upper hand. At the highest level, the state must recognize that fraud not only has a financial cost for its victims but a deleterious effect on their trust in institutions. Alongside updates to legislation, the state can boost the role of defensive tech by ensuring it has adequate backing and accountability. For example, companies involved in telecommunications, internet provision or other tech services used by scammers should be mandated to follow state-set cybersecurity standards for their customers, or face fines or punishment. But the state also has a role to play in educating citizens about their own responsibilities, including though the adoption of tech that helps combat fraud (such as Truecaller, which screens out scam calls).

The centrality of technology in people's lives makes it critical that public awareness does not only cover what not to do, but what to do. This will create a world in which personal cybersecurity tools are not seen as an 'added extra' but a form of digital health insurance. In May 2025, the National Bank of Ukraine launched Goodbye Scammer, a mass public awareness campaign about how citizens should improve their own cybersecurity.[180] This initiative has many innovative features, such as a newspaper for older people and educational events for younger people. But it is scheduled to last only until the end of 2025.[181] A longer-term strategy, such as permanently building cybersecurity literacy into educational curricula, is required to cope with the seismic shift to life online.

NOTES

1 Interview with police, Kyiv, September 2024. The most widespread crimes in Ukraine are economic crime, call centres, drugs and people smuggling.

2 Ukrainian Interbank Payment Systems Member Association (EMA) presentation shared with the GI-TOC.

3 Interview with an EMA representative, Kyiv, July 2025.

4 Ibid.

5 Based on figures provided in an interview with an MP, Kyiv, February 2025.

6 Interview with an MP, Kyiv, February 2025.

7 For supporting evidence of this claim, see pp 13–14 of this report.

8 GI-TOC survey of open-source media in Ukrainian, Russian and English.

9 Ukrainian official's response to a question during a UN Office on Drugs and Crime (UNODC) event, Kyiv, July 2025.

10 Ibid.

11 Prosecutor General's Office, The Prosecutor General's Office conducted another large-scale special operation to expose the activities of fraudulent call centers, 31 December 2025, https://gp.gov.ua/en/posts/ofis-generalnogo-prokurora-proviv-cergovu-masstabnu-specoperaciyu-iz-vikrittya-diyalnosti-saxraiskix-kol-centriv.

12 UNN, Special operation "Connect": Ukraine and the EU liquidated a transnational network of fraudulent call centres, 16 December 2025, https://unn.ua/en/news/special-operation-connect-ukraine-and-the-eu-liquidated-a-transnational-network-of-fraudulent-call-centers.

13 Federal Trade Commission, Anticipating the 21st century: Consumer protection policy in the new high-tech, global marketplace, May 1996, p 3, https://www.ftc.gov/system/files/documents/reports/anticipating-21st-century-competition-policy-new-high-tech-global-marketplace/gc_v2.pdf. For a list of prominent 1990s scams see Verizon, Consumer scams, https://www.verizon.com/business/solutions/public-sector/federal-government/contracts/wits3/customer-care/telecom-security-fraud-prevention/consumer-scams; and Washington State (Office of Attorney General), AG warns consumers to avoid phone card pyramid scheme, 12 February 1996, https://www.atg.wa.gov/news/news-releases/ag-warns-consumers-avoid-phone-card-pyramid-scheme. See also Diana B Henriques, Investing: The scam goes on, *The New York Times*, 23 September 1990, https://www.nytimes.com/1990/09/23/magazine/investing-the-scam-goes-on.html.

14 Charles Arthur, Virus phone scam being run from call centres in India, *The Guardian*, 18 July 2010, https://www.theguardian.com/world/2010/jul/18/phone-scam-india-call-centres.

15 OCCRP, Everything you need to know about 'scam empire', 5 March 2025, https://www.occrp.org/en/project/scam-empire/scam-empire-everything-you-need-to-know-about-these-massive-investment-scams; Simona Weinglass, Israeli government unveils draft law to ban binary options, *Times of Israel*, 24 February 2017, https://www.timesofisrael.com/israeli-government-unveils-draft-law-to-ban-binary-options.

16 Interview with iFact, Tbilisi, March 2025; Georgy Ak-Murza, How to steal by phone: features of call centres, Dumskaya, 3 December 2024, https://dumskaya.net/news/noveyshie-metody-vliyaniya-seminary-s-psihologam-186630/ua.

17 OCCRP, Web of call-centre scammers reaches into Albania, Georgia, 6 March 2020, https://www.occrp.org/en/project/fraud-factory/web-of-call-center-scammers-reaches-into-albania-georgia; OCCRP, Trail of broken lives leads to Kyiv call centre, 2 March 2020, https://www.occrp.org/en/project/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center.

18 OCCRP, Trail of broken lives leads to Kyiv call centre, 2 March 2020, https://www.occrp.org/en/project/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center.

19 In Russia, Dnepr has been called the 'capital of telephone fraud', *Ukrainska Pravda*, 3 October 2021, https://www.pravda.com.ua/rus/news/2021/10/3/7309204.

20 Interview with former call centre employee S, Kyiv, January 2025.

21 Maksym Zaychenko, In the Kherson region, prisoners set up a fraudulent call centre in a pre-trial detention centre, Informator, 23 September 2021, https://informator.ua/uk/u-hersonskiy-oblasti-uv-yazneni-oblashtuvali-shahrayskiy-koll-centr-v-sizo. Another prison call centre was discovered in 2023 in Vinnytsia. Yaroslava Borzova, 'Earned' UAH 2 million per month: Prison convicts defrauded tens of thousands of Ukrainians, RBC,

27 November 2023, https://www.rbc.ua/rus/news/vinnitskiy-oblasti-vikrili-feykoviy-sall-1701094388.html.

22 EMA presentation shared with the GI-TOC, citing Cyber Police data.

23 Ibid.

24 Interview with an EMA representative, Kyiv, July 2025.

25 Telephone scams in 2023, Finance.ua, 9 March 2023, https://finance.ua/ua/goodtoknow/telefonni-szahrajstva-2023; Prosecutor's Office, Relatives of military personnel who went missing or were captured were defrauded of UAH3 million – a group of individuals was exposed in the Dnipropetrovsk region, 3 June 2025, https://www.gp.gov.ua/ua/posts/osukali-na-3-mln-grn-rodiciv-viiskovix-yaki-znikli-bezvisti-ci-potrapili-v-polon-na-dnipropetrovshhini-vikrito-grupu-osib; Mykola Tyshchenko, Ботоферма обікрала на 7,5 мільйонів гривень матір Героя, що загинув, захищаючи Україну, Telegram, https://t.me/NikolayTishchenko/1789; Polina Snezhina, Man who defrauded the mother of a deceased soldier of almost UAH150 000: imprisoned man to be tried in Zaporizhia, Suspilne, 17 June 2025, https://suspilne.media/zaporizhzhia/1045025-osukav-matir-zagiblogo-vijskovogo-majze-na-150-tis-grn-u-zaporizzi-suditimut-uvaznenogo-colovika.

26 Anastasia Chebrets, 'Agent Nimets' and its call centre 'E-Scam' in Lviv, Informator, 6 September 2023, https://informators.press/ahent-nimets-i-yoho-kol-tsentr-ye-shakhraystvo-u-lvovi/; How scammers steal military fees: common schemes, Espresso West, 29 February 2024, https://zahid.espreso.tv/kryminal-nadsilati-groshi-lishe-tomu-komu-doviryaemo-yak-shakhrai-kradut-zbori-dlya-viyskovikh-i-privlasnyuyut-sobi-groshi.

27 Oleg Bessarab, Fraudsters in Ukraine have come up with a new scheme, intimidating with treason – police, UA.News, 18 May 2025, https://ua.news/ua/ukraine/shahrayi-v-ukrayiny-prydumaly-novu-shemu-zalyakuyuchy-derzhzradoyu-politsiya.

28 Mykola Tyshchenko, Very unpleasantly surprised. Racist bot farm in the centre of ... Uzhhorod, Telegram, https://t.me/NikolayTishchenko/1777.

29 Since the beginning of the war, the number of frauds has increased, not all victims are ready to talk about them publicly – lawyer, Interfax, 4 February 2025, https://interfax.com.ua/news/general/1045448.html; Olena Demina, Cryptocurrency fraud: 4 new schemes that emerged during the war, MinFin, 29 March 2022, https://minfin.com.ua/ua/2022/03/29/82848509.

30 Openness of Professions, Earned $6,000 in a week – Dnipro offices. How call centres work, YouTube, 28 September 2023, https://www.youtube.com/watch?v=KlRwhjqjY6g, 0:57.

31 Kateryna Shapoval, Golden 'offices'. In Ukraine – thousands of fraudulent call centres are defrauding tens of millions of dollars a year (mostly from Russians). How this industry works. A major Forbes study, *Forbes*, 6 December 2024, https://forbes.ua/company/skhema-makroekonomichnogo-zrostannya-03122024-25236; Working in the 'office'. How people are employed in fraudulent call centres, *Economic Pravda*, 24 March 2023, https://epravda.com.ua/publications/2024/07/16/716741; Christina Sizova, Welcome to Ukraine's secret offensive: They scam, bankrupt, and drive Russian civilians to suicide, RT, 25 February 2025, https://www.rt.com/russia/613275-ukraine-phone-scammers-deceive-russians.

32 Bovtruk and Retz, Right next to the SBU. How call centres operate in Ukraine, ripping off Russian bank clients, Strana, 30 September 2021, https://strana.best/articles/rassledovania/355432-kak-rabotajut-v-ukraine-koll-tsentry-kotorye-razvodjat-na-denhi-klientov-rossijskikh-bankov.html.

33 Interview with former call centre employee L, February 2025.

34 Interview with an EMA representative, Kyiv, July 2025.

35 New wave of military registration and enlistment office arson attacks in Russia. Detainees blame phone scammers, BBC Russia, 1 August 2023, https://www.bbc.com/russian/articles/c3g1zxdnd3wo; Alexey Voloshinov, "Mediazona": In the Russian Federation - the largest wave of arson since the beginning of the war, DW, 25 December 2024, https://amp.dw.com/ru/mediazona-v-rossii-samaa-krupnaa-volna-podzogov-s-nacala-vojny/a-71155791.

36 Putin: telephone fraud in Ukraine has been elevated to the level of state policy, TASS, 10 December 2024, https://tass.ru/politika/22631303.

37 Georgy Ak-Murza, How to steal by phone: features of call centres, Dumskaya, 3 December 2024, https://dumskaya.net/news/noveyshie-metody-vliyaniya-seminary-s-psihologam-186630/ua.

38 Valeria Chepurko, Maksym Buzhansky: Calls from prisons are childish babbling compared to modern call centres, KP.ua, 11 August 2023, https://kp.ua/ua/incidents/a674539-maksim-buzhanskij-dzvinki-z-vjaznits-ditjachij-belkit-u-porivnjanni-z-suchasnimi-kol-tsentrami.

39 Interview with an MP who worked on call centre commission, February 2025.

40 EMA presentation shared with the GI-TOC.

41 Olga Paliy, Thousands of 'employees', bribes, crypt and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikiv-habari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-v-ukrajini; Anti-Corruption Human Rights Council, Call centres: fraud in Ukraine, 20 October 2023, https://com1.org.ua/koll-tsentry-shakhrajstvo-v-ukraini; Yaroslav Dmytrenko, Call centres. Business and nothing personal, Osoby, 25 December 2023, https://www.osoby.com.ua/kol-czentry-biznes-ta-nichogo-osobystogo; In a day, the SBU and the National Police eliminated over 100 fraudulent call centres that stole personal data and money from Ukrainians, SBU, 29 December 2023, https://ssu.gov.ua/novyny/za-dobu-sbu-ta-natspolitsiia-likviduvaly-ponad-100-shakhraiskykh-calltsentriv-yaki-vykradaly-personalni-dani-ta-hroshi-ukraintsiv; interview with an MP, Kyiv, February 2025.

42 Interview with an EMA representative, Kyiv, July 2025: 'As a rule, a call centre is 20, 30, 40 people – let's say it's the average. But if we take the average figure here and multiply it by 2 000, then we

will get the same number of employees as we have in the banking sector of Ukraine.' This may be an exaggeration. Taking 30 as the average size gives a total call centre headcount of 60 000, against a banking headcount of 96 000 in April–June 2024. The pre-invasion banking headcount was reportedly 210 000; Ukrainian banks reduce number of staff – NBU review, Interfax, 16 August 2024, https://interfax.com/newsroom/top-stories/105183/; Raising Ukraine's productivity: banking sector as an engine for growth, McKinsey & Company, March 2016, https://www.mckinsey.com/ua/~/media/ClientLink/Raising%20Ukraines%20productivity%20Banking%20sector%20as%20an%20engine%20for%20growth/Ukraine%20productivity%20growth_EN_web.pdf.

43 GI-TOC, Dnipro: The front line of crime, July 2025, https://globalinitiative.net/analysis/dnipro-the-front-line-of-crime.

44 GI-TOC, Odesa: An oasis for organized crime, April 2025, https://globalinitiative.net/analysis/odesa-an-oasis-for-organized-crime; GI-TOC, Smuggling, Inc.: Illicit trade between Ukraine's Transcarpathia and the EU, April 2025, https://globalinitiative.net/analysis/illicit-trade-between-ukraines-transcarpathia-and-the-eu.

45 GI-TOC open-source survey of Ukrainian-language media concerning instances of call centres operating since February 2022.

46 LPR lawyer, Beware of telephone scammers!, Dzen, 12 February 2023, https://dzen.ru/b/Y-iYo7b7bh7QWXLB.

47 Interview with an MP, Kyiv, February 2025.

48 Online scams may already be as big a scourge as illegal drugs, *The Economist*, 6 February 2025, https://www.economist.com/briefing/2025/02/06/online-scams-may-already-be-as-big-a-scourge-as-illegal-drugs.; A senior law enforcement official in Kyiv said call centres are the second biggest illicit market in Ukraine, after economic crime, interview, Kyiv, September 2024.

49 Interview with S, Kyiv, January 2025.

50 See: https://www.tiktok.com/@scamline.office/video/7507639524017753400?; https://www.tiktok.com/@top_company_kiev. The TikTok page has short videos aimed at attracting potential employees, who are asked to message the company's Telegram account (which has no posts).

51 Interview with an EMA representative, Kyiv, July 2025.

52 The pre-trial investigation established that the Solomianskyi UP of the main directorate of the National Police in Kyiv received information about the operation of call centres in the Solomianskyi district of Kyiv, in particular at the following addresses: 1-A Vadyma Hetmana St (1st floor); 1-V Vadyma Hetmana St (3rd floor); 154 Borshchahivska St, Marmelad shopping centre (3rd, 4th, 5th and top floors); 192 Borshchahivska St, BC Bizon (5th–7th floors); 2/1 Mykoly Hrinchenka St, BC 'Protasiv Yar'; 26/8 Metalistiv St (6th and 7th floors); 6 Vadyma Hetmana St; (building A), Cosmopolit (4th–6th floors), building C (6th floor); 12 Amosova St, BC Horizon Park (building 2, floor 8); 24 Polyova St; 11 Solomyanska St (offices 33122, 33123, 33124, 34045), https://opendatabot.ua/court/113755670-447f218b240291db6fbe07c7b7614ae6.

53 Interview with S, Kyiv, January 2025.

54 Interview with law enforcement #1, Transcarpathia, May 2025.

55 Maria Yemets, Czech police, together with the SBU, exposed a call centre in Transcarpathia that was deceiving Europeans, Eurointegration, 13 May 2025, https://www.eurointegration.com.ua/news/2025/05/13/7211482; Natalia Kava, A call centre was exposed in Transcarpathia, whose employees were extorting money from EU citizens, RBC, 5 June 2024, https://www.rbc.ua/rus/news/zakarpatti-vikrili-call-tsentr-pratsivniki-1717593546.html; Ministry of Internal Affairs of Ukraine, Transcarpathian police shut down another fraudulent call centre, 25 October 2023, https://mvs.gov.ua/news/policiia-zakarpattia-likviduvala-cergovii-saxraiskii-call-centr-video; Mykhailo Pylypko, In Chop, police uncovered a call centre with over 30 operators working there, 7 December 2023, Suspilne, https://suspilne.media/uzhhorod/634242-u-copi-policejski-vikrili-call-centr-v-akomu-pracuvali-ponad-30-operatoriv; A large-scale network of fraudulent call centres, through which 17 foreigners were defrauded of almost $1 million, was dismantled in Transcarpathia, Zakarpattya, 5 June 2024, https://zakarpattya.net.ua/News/233526-Na-Zakarpatti-likviduvaly-masshtabnu-merezhu-shakhraiskykh-kol-tsentriv-cherez-iaku-vymanyly-v-17-inozemtsiv-maizhe-$1-milion-FOTO; Anna Semenyuk, Operators of a fraudulent call centre in Uzhhorod were defrauding foreigners of $500 000 every month, Zaxid, 24 March 2023, https://zaxid.net/operatori_shahrayskogo_kol_tsentru_v_uzhgorodi_vimanyuvali_v_inozemtsiv_500_tis_shhomisyatsya_n1560433; Kateryna Petruno, A call centre whose organizers are suspected of fraud of over $130,000 has been shut down in Uzhhorod, Suspilne, 24 March 2023, https://suspilne.media/uzhhorod/424074-v-uzgorodi-pripinili-dialnist-kol-centru-organizatoriv-akogo-pidozruut-u-sahrajstvi-na-ponad-130-dolariv; Angelica Baibak, 'Tyshchenko's fighting method': Armed men who attacked a call centre were detained in Uzhhorod, 24tv, 23 August 2024, https://24tv.ua/uzhgorodi-nevidomi-napali-kol-tsentr-shho-vidomo-pro-intsident_n2625195; In Uzhhorod, police uncovered a call centre that was extorting money from citizens of the Czech Republic and Hungary, Zaholovok, 11 August 2023, https://zaholovok.com.ua/v-uzhhorodi-politsiya-vykryla-kol-tsentr-yakyy-vymanyuvav-hroshi-vid-hromadyan-chekhiyi-ta.

56 This rationale for Chop was provided by a law enforcement source in Transcarpathia. Interview with law enforcement #2, Transcarpathia, May 2025.

57 The association of the account with scam call centres is suggested by content in the videos. For instance, one caption says 'When a closer closes your phone handset [client]' to a video of two workers dancing.

58 Another indication of the real activity of the call centre is from the TikTok account of this centre. In one video, the caption (in Russian) says 'When your girl closes a [emoji of a mammoth = victim] for 10 mil and you brought her in just a week ago'.

59 Rieltor listing, Levka Lukyanenka St (Marshalf Tymoshenkf), 21/14, https://rieltor.ua/commercials-rent/view/11938838.

60 Interview with L, February 2025.

61 Georgy Ak-Murza, How to steal by phone: features of call centres, Dumskaya, 3 December 2024, https://dumskaya.net/news/noveyshie-metody-vliyaniya-seminary-s-psihologam-186630/ua.

62 Interview with an EMA representative, Kyiv, July 2025.

63 Interview with L, February 2025.

64 Ibid.

65 Slonets Bohdan, Police found a scam call centre in Rivne, Rivne Post, 1 January 2024, https://rivnepost.rv.ua/news/politsiya-znayshla-u-rivnomu-koltsentr-shakhraiv-video; National Police of Ukraine, The National Police dismantled a large-scale network of fraudulent call centres with billions in turnover, YouTube, 29 December 2023, https://www.youtube.com/watch?v=KHcqswBkcMs; interview with EMA, Kyiv, July 2025.

66 UNODC, Ukraine: Organized crime dynamics in the context of war, July 2025, https://www.unodc.org/documents/data-and-analysis/Ukraine/Ukraine_OC_Study.pdf. According to the UNODC, the 'call centres "industry" is dominated by five criminal groups, each operating at least 10 call centres. Khimprom and Dniprovski [Dnipro networks] have been named as the two largest groups in this illicit market.' This may still tally with the GI-TOC's assessment, which includes the diverse Dnipro networks as one 'cluster' of criminal involvement.

67 Interview with L, February 2025.

68 National Police of Ukraine, The National Police exposed the organizers of an international fraudulent scheme with a monthly turnover of UAH 5 million, YouTube, 16 March 2023, https://www.youtube.com/watch?v=JGh9osGvJeo.

69 An *avtoritet* – literally translated as 'authority' – may work in both the legal and illegal economy and has no hesitation in cooperating with the state, unlike a thief-in-law. For more on the connections between Oliynyk and Petrovsky, including their alleged involvement in criminal activity, see GI-TOC, Dnipro: The front line of crime, July 2025, https://globalinitiative.net/analysis/dnipro-the-front-line-of-crime.

70 Interview with L, February 2025.

71 Yaroslav Kodzhushko, Attack on ex-military man in Dnipro: after acquittal in the Rada, Tyshchenko said he had exposed the fraudsters, Informator, 21 June 2024, https://informator.ua/uk/napad-na-eksviyskovogo-u-dnipri-pislya-vipravdan-u-radi-tishchenko-zayaviv-shcho-vikriv-shahrajiv.

72 Interview with an MP, February 2025; Jack Meegan-Vickers, Scam call centres in Ukraine, GI-TOC, 21 October 2023, https://globalinitiative.net/analysis/scam-call-centres-in-ukraine; Oleg Shevchenko, The organizer of a drug syndicate with the support of the FSB 'turned around' in Ukraine: he is wanted, but runs from abroad, Obozrevatel, 4 April 2023, https://incident.obozrevatel.com/ukr/crime/organizator-narkosindikatu-za-pidtrimki-fsb-rozvernuvsya-v-ukraini-vin-u-rozshuku-ale-kerue-z-za-kordonu.htm.

73 SBU, The SBU blocked the activities of a 'unit' of the international drug syndicate 'Khimprom', 8 October 2020, https://ssu.gov.ua/novyny/cbu-blokuvala-diialnist-pidrozdilu-mizhnarodnoho-narkosyndykatu-khimprom-video.

74 Russia: Call centre scheme that deceived hundreds from over 20 countries exposed in Moscow, TASS, 11 December 2024, https://tass.com/society/1885619; interview with an MP, Kyiv, February 2025.

75 Cyber Police officer allegedly covered up a black call centre with 500 people. Received $16,000. Investigation underway, Dev, 1 March 2024, https://dev.ua/news/kiberpolitsai-1709304656; Anti-Corruption Human Rights Council. Call centres: fraud in Ukraine, 20 October 2023, https://com1.org.ua/koll-tsentry-shakhrajstvo-v-ukraini.

76 Interview with S, Kyiv, January 2025.

77 Interview with an MP, Kyiv, February 2025.

78 Interview with S, January 2025.

79 Interviews with former call centre employees S, A1 and L, January–February 2025.

80 Interview with A1, February 2025.

81 Interview with L, February 2025.

82 Interview with an MP, Kyiv, February 2025.

83 Valeria Chepurko, Maksym Buzhansky: Calls from prisons are childish babbling compared to modern call centres, KP.ua, 11 August 2023, https://kp.ua/ua/incidents/a674539-maksim-buzhanskij-dzvinki-z-vjaznits-ditjachij-belkit-u-porivnjanni-z-suchasnimi-kol-tsentrami.

84 Interview with an MP, Kyiv, February 2025: 'We received docs showing the numbers and the recipients in law enforcement (US$10 000–US$15 000 a month). We had information about call centres contacting all law enforcement agencies.' In another media report, the figure of US$12 000 a month was mentioned; Olga Paliy, Thousands of 'employees', bribes, crypt and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikiv-habari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-v-ukrajini.

85 Interview with an MP, Kyiv, February 2025.

86 According to the investigation, scammers at the Milton Group assessed potential victims by country: 'South Africans were easy targets and good for novice salespeople to practise on, while British people were harder sells and required a "strong" touch.' OCCRP, Web of call-centre scammers reaches into Albania, Georgia, 6 March 2020, https://www.occrp.org/en/project/fraud-factory/web-of-call-center-scammers-reaches-into-albania-georgia.

87 Interview with L, February 2025.

88 Interview with investigative journalist researching call centres, June 2025. A language teacher said she had been approached by a call centre to teach scammers Czech and Slovak. Adverts have also appeared in Ukrainian looking for a Hungarian language teacher.

89 Interview with L, February 2025; Ministry of Internal Affairs of Ukraine, Cyber police expose organizers of fraudulent call centre who misappropriated cryptocurrency assets of

foreigners, 21 June 2023, https://mvs.gov.ua/news/kiberpoliciia-vikrila-organizatoriv-saxraiskogo-call-centru-iaki-privlasnili-kriptovaliutni-aktivi-inozemciv.

90 Olga Paliy, Thousands of 'employees', bribes, crypt and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikiv-habari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-v-ukrajini.

91 See, for instance, this maxim repeated in the Russian context in Alexey Malov, Confessions of a carder, 2 March 2010, The Literature Network Forums, https://www.online-literature.com/forums/showthread.php?51245-Confessions-of-a-carder-by-russian-writer.

92 To take two cases that have been under investigation for years: a case involving Swiss citizens, under which a task force was created in January 2022; the last update on the case in the judicial register came in August 2024 (https://reyestr.court.gov.ua/Review/118868568). See also the case of a call centre first investigated in November 2022 that was still under investigation in May 2025 (https://reyestr.court.gov.ua/Review/127546152).

93 Companies House, https://find-and-update.company-information.service.gov.uk/officers/4lTXR_2cf17k4EjXkQCU6eRygx4/appointments. Both appointments of Blockchain Ltd had been struck off the list of UK companies in November 2019, before the scam was perpetrated.

94 Foreign citizens' cryptocurrency assets were misappropriated: National Police of Ukraine, Cyber Police exposed the organizers of a fraudulent call centre, 21 June 2023, https://npu.gov.ua/news/pryvlasnyly-kryptovaliutni-aktyvy-inozemnykh-hromadian-kiberpolitsiia-vykryla-orhanizatoriv-shakhraiskoho-call-tsentru; Criminal case 12023240000000036, 7 December 2023, https://reyestr.court.gov.ua/Review/112141905.

95 Victoria Podorozhnaya, Vikrito Shakhrai call centre, which has benefited the residents of Canada, Korespondent, 21 June 2023, https://ua.korrespondent.net/ukraine/4600280-vykryto-shakhraiskyi-call-tsentr-yakyi-oshukuvav-zhyteliv-kanady.

96 Criminal case 12023240000000036 resolution, 20 August 2023, https://reyestr.court.gov.ua/Review/112915240.

97 Criminal case 12023240000000036 resolution, 22 June 2023, https://reyestr.court.gov.ua/Review/111697849; Criminal case 12023240000000036 resolution, 20 August 2023, https://reyestr.court.gov.ua/Review/112915240; Criminal case 12023240000000036 resolution, 8 August 2023, https://reyestr.court.gov.ua/Review/113026573; Criminal case 12023240000000036 resolution, 13 July 2023, https://reyestr.court.gov.ua/Review/112141905.

98 Criminal case 12023240000000036 resolution, 20 November 2023, https://reyestr.court.gov.ua/Review/115007111.

99 Criminal case 12023240000000036 resolution, 12 July 2023, https://reyestr.court.gov.ua/Review/112141905.

100 Interview with an EMA representative, Kyiv, July 2025.

101 Cyber Police, Scammers call and offer to install a new bank app: what is the purpose of the fraudulent scheme?, 28 April 2025, https://cyberpolice.gov.ua/article/shaxrayi-telefonuyut-ta-proponuyut-vstanovyty-novyj-zastosunok-banku-yaka-meta-shaxrajskoyi-sxemy-5159; Cyber Police, About 1.4 million UAH in losses: Dnipropetrovsk region police neutralized a fraudulent criminal organization, 11 July 2025, https://cyberpolice.gov.ua/news/blyzko--mln-grn-zbytkiv-policzejski-dnipropetrovshhyny-zneshkodyly-shaxrajsku-zlochynnu-organizacziyu-2109.

102 Lyuba Balashova, An application for 19 million Ukrainians. Fraudsters are forging 'Diya' to travel abroad, steal bank details, and defraud stores. How not to get caught?, *Forbes*, 5 November 2023, https://forbes.ua/innovations/dodatok-na-19-mln-shakhrai-pidroblyayut-diyu-dlya-otrimannya-paroliv-vid-kartok-ta-viizdu-za-kordon-yak-ne-potrapiti-na-gachok-02112023-17007; Digital State UA, https://digitalstate.gov.ua/projects/govtech/diia.

103 Briefing: Prominent Russian data-leak tool suspended under new personal data law, BBC Monitoring, 4 March 2025, https://monitoring.bbc.co.uk/product/b0003gh2#.

104 GI-TOC, Odesa: An oasis for organized crime, April 2025, https://globalinitiative.net/analysis/odesa-an-oasis-for-organized-crime; Polina Snezhina, EU citizens were defrauded: two employees of a fraudulent call centre will be tried in Zaporizhia, Suspilne, 9 July 2025, https://suspilne.media/zaporizhzhia/1062267-osukali-gromadan-es-u-zaporizzi-suditimut-dvoh-pracivnikiv-sahrajskogo-kol-centru.

105 Europol, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests, 24 November 2022, https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-'spoofing'-services-to-fraudsters-142-arrests.

106 Interview with an EMA representative, Kyiv, July 2025; Whitelist (allowed list): important information for regular users, Plisio, 19 May 2024, https://plisio.net/uk/blog/whitelist-allowlist; Require strong passwords, US Cybersecurity and Infrastructure Security Agency (CISA), https://www.cisa.gov/secure-our-world/require-strong-passwords; Create and use strong passwords, Microsoft, https://support.microsoft.com/en-gb/windows/create-and-use-strong-passwords-c5cebb49-8c53-4f5e-2bc4-fe357ca048eb. On passwords, Microsoft recommends at least 14 characters, and CISA recommends at least 16 characters.

107 Interview with S, Kyiv, January 2025: 'Call centres promising "wow" conditions are usually worse in reality.'

108 GI-TOC, Compound crime: Cyber scam operations in southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia.

109 Interview with A1, February 2025. According to another HR manager, people between 20 and 30 are preferred. Interview with L, February 2025.

110 Olga Paliy, Thousands of 'employees', bribes, crypt and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikiv-habari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-v-ukrajini.

111 Interview with a former call centre employee A2, April 2025.

112 Interview with L, February 2025.
113 Interview with A1, February 2025.
114 Interview with S, Kyiv, January 2025.
115 Interview with A2, April 2025.
116 Ibid.
117 Interview with L, February 2025.
118 Interview with A1, February 2025.
119 Interview with A1 and L, February 2025. (Both cited UAH100 000 a day, A1 cited UAH300 000 a week).
120 Interview with L, February 2025.
121 Interviews with S and A1, January and February 2025.
122 Interview with A1, February 2025.
123 Nina Day, Everything you wanted to ask a call centre operator but were too shy to ask, 1 August 2019, VCTR, https://vctr.media/ua/tizhkoltsentr-25729.
124 Interview with A1, February 2025.
125 Interview with an EMA representative, Kyiv, July 2025.
126 Interview with S, Kyiv, January 2025.
127 Interview with A1, February 2025.
128 Interview with L, February 2025.
129 Interview with A1, February 2025: 'An experienced worker tr[ied] to get out and leave. This provoked a negative reaction, they finished their conversation on a bad note, as a result by the end of the day he was beaten and continued to work.'; Olga Paliy, Thousands of 'employees', bribes, crypt and torture: how fraudulent call centres in Ukraine are organized, Informator, 26 July 2023, https://informator.ua/uk/tisyachi-spivrobitnikiv-habari-kripta-ta-torturi-yak-vlashtovani-shahrayski-kol-centri-v-ukrajini.
130 Interview with L, February 2025.
131 Interview with A2, April 2025.
132 Interview with L, February 2025.
133 Interview with A1, February 2025.
134 Interview with L, February 2025.
135 Ibid.
136 Ibid.
137 Interview with an EMA representative, Kyiv, July 2025.
138 Yulia Feshchenko, Not just instant messenger hacking and phishing. Experts have named common banking fraud schemes, MC Today, 19 December 2024, https://mc.today/uk/ne-tilki-zlam-mesendzheriv-ta-fishing-eksperti-nazvali-poshireni-shemi-bankivskogo-shahrajstva.
139 Interview with an EMA representative, Kyiv, July 2025.
140 Ibid.
141 Ibid.
142 Interview with MP, Kyiv, February 2025.
143 Ibid.
144 'In 2024, due to the mass departure of young people, the number of call centres began to decline.' Georgy Ak-Murza, How to steal by phone: features of call centres, Dumskaya, 3 December 2024, https://dumskaya.net/news/noveyshie-metody-vliyaniya-seminary-s-psihologam-186630/ua.
145 Ukrainian official's response to question during a UNODC event, Kyiv, 2025.
146 Volodymyr Pyrih, The government has banned detainees from ordering paid internet access in pre-trial detention centres, Zaxid, 9 October 2023, https://zaxid.net/uryad_zaboroniv_zatrimanim_zamovlyati_platniy_dostup_do_internetu_v_sizo_n1572303; Kateryna Beniuk, Military personnel and their families are targeted by scammers. How to protect yourself, Zahid, 23 September 2024, https://zahid.espreso.tv/suspilstvo-chomu-shakhrai-natsilyuyutsya-na-viyskovikh-i-ikhni-simi-ta-yak-vid-nikh-zakhistitisya.
147 Andrey Annenkov, On the 'ban on IP telephony in Russia' – what does the change in the rules for licensing telecom operators mean, D-Russia, 28 December 2024, https://d-russia.ru/o-zaprete-ip-telefonii-v-rossii-chto-oznachaet-izmenenie-pravil-licenzirovanija-operatorov-svjazi.html.
148 Oleg Davydov, The State Duma assessed the likelihood of blocking Telegram, Lenta, 5 June 2025. https://lenta.ru/news/2025/06/05/v-gosdume-otsenili-veroyatnost-blokirovki-telegram.
149 Interview with A2, April 2025: 'Now there are fewer ads – it has been declining since 2024–25. There were a lot of them in 2022–23. Such ads are usually very colourful, lively, they try to attract attention, they use a lot of smileys. Telegram channels have the most ads.'
150 Layboard adverts, https://layboard.com/ua/vakansiya/615680/operator-kol-centr and https://layboard.com/ua/vakansiya/1536781/rabota-v-ofise; Georgy Ak-Murza, How to steal by phone: features of call centres, Dumskaya, 3 December 2024, https://dumskaya.net/news/noveyshie-metody-vliyaniya-seminary-s-psihologam-186630/ua: 'Ukrainian call centres have become quite noticeably more active in European countries, where they mostly specialize in refugees. To do this, operators present themselves as employees of some "Ukrainian" police departments or migration services of EU countries and skilfully imitate the accent when communicating with victims.'
151 Interview with L, February 2025.
152 Layboard advert, https://layboard.com/vakansiya/1546151/sales-manager.
153 Interview with an EMA representative, Kyiv, July 2025.
154 Ksenia Hassan, Fraudulent call centre in Canyon Business Centre with Filipino-British roots: Police launch pre-trial investigation, StopCor, 19 February 2025, https://www.stopcor.org/ukr/section-suspilstvo/news-shahrajskij-kol-tsentr-u-bts-kanjon-z-filipinsko-britanskim-korinnyam-politsiya-rozpochala-dosudove-rozsliduvannya-19-02-2025.html; Halyna Khomulyak, In Kyiv, journalists exposed a scam office in the prestigious Mikom Palace business centre, Stopcor, 29 April 2025, https://www.stopcor.org/ukr/section-suspilstvo/news-u-kievi-zhurnalisti-vikrili-skam-ofis-u-prestizhnomu-biznes-tsentri-mikom-palace-29-04-2025.html; Galina Khomulak, A fraudulent call centre with English-speaking administrators was exposed in the capital's Solomenka, StopCor, 5 February 2025, https://www.stopcor.org/section-

uanews/news-na-stolichnij-solomyantsi-vikrili-shahrajskij-kol-tsentr-z-anglomovnimi-administratorami-foto-05-02-2025.html; police document seen by the GI-TOC.

155 Interview with an MP, Kyiv, February 2025.

156 Interview with an EMA representative, Kyiv, July 2025.

157 Interview with a journalist, Odesa, July 2025.

158 Cyber Police contribution to discussion at a UNODC event in Kyiv, July 2025.

159 Anyone can become a fraudster for just 300 euros, Financial Club, 5 June 2024, https://finclub.net/news/shakhraiem-mozhe-staty-kozhen-lyshe-za-300-ievro.html.

160 Interview with an EMA representative, Kyiv, July 2025.

161 Ibid.

162 Alan Blackmore, The death of the call centre: How voice AI is transforming inbound and outbound call operations, Medium, 18 March 2025, https://alanblackmore.medium.com/the-death-of-the-call-centre-how-voice-ai-is-transforming-inbound-and-outbound-call-operations-77392c663be6.

163 Interview with an EMA representative, Kyiv, July 2025.

164 Valeria Chepurko, Maksym Buzhansky: Calls from prisons are childish babbling compared to modern call centres, KP.UA, 11 August 2023, https://kp.ua/ua/incidents/a674539-maksim-buzhanskij-dzvinki-z-vjaznits-ditjachij-belkit-u-porivnjanni-z-suchasnimi-kol-tsentrami.

165 Ibid.

166 Scam call centres from Ukraine defrauded 33 000 people from around the world of $275 million, MinFin, 7 March 2025, https://minfin.com.ua/ua/crypto/articles/skamerskie-kollcentry-iz-ukrainy-obmanuli-33-tys-lyudey-so-vsego-mira-na-275-mln.

167 Interview with an MP, Kyiv, February 2025.

168 Ibid.

169 UNN, "From words to deeds": Kravchenko reported on the exposure of a scheme for fraudsters to profit from EU citizens for about $250 thousand within the framework of international cooperation, 21 November 2025, https://unn.ua/news/vid-sliv-do-sprav-kravchenko-povidomyv-pro-vykryttia-u-mezhakh-mizhnarodnoi-spivpratsi-shakhraiv-yaki-oshukaly-hromadian-yes-na-dollar250-tysiach.

170 Tyshchenko returned to the Verkhovna Rada, UkraNews, 8 January 2025, https://ukranews.com/ua/news/1057348-tyshhenko-povernuvsya-u-verhovnu-radu.

171 Kateryna Beniuk, Military personnel and their families are targeted by scammers. How to protect yourself, Zahid, 23 September 2024, https://zahid.espreso.tv/suspilstvo-chomu-shakhrai-natsilyuyutsya-na-viyskovikh-i-ikhni-simi-ta-yak-vid-nikh-zakhistitisya.

172 Cyber Police, In 2024, police are implementing new strategies to combat fraudulent schemes, 19 January 2024, https://cyberpolice.gov.ua/news/u--roczi-policzejski-vprovadzhuyut-novi-strategiyi-protydiyi-shaxrajskym-sxemam-3324.

173 Interview with an Armenian NGO, March 2025.

174 Interview with Canadian law enforcement, July 2025.

175 Europol, International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war, 28 November 2023, https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war.

176 Council of Europe, C-PROC delegates attend the Annual Conference of the European Cybercrime Centre (EC3), 18–19 October 2023, https://www.coe.int/en/web/cybercrime/-/c-proc-delegates-attend-the-annual-conference-of-the-european-cybercrime-centre-ec3-.

177 Nafis Nebarjadi and Amanda Storey, The new Global Signal Exchange will help fight scams and fraud, Google Blog, 9 October 2024, https://blog.google/technology/safety-security/the-new-global-signal-exchange-will-help-fight-scams-and-fraud.

178 Interview with Canadian law enforcement, July 2025.

179 Interview with an EMA representative, Kyiv, July 2025; Will WhatsApp and Telegram be blocked to promote the national messenger Max?, Verstka, 18 July 2025, https://verstka.media/whatsapp-telegram-zablokiruit-li-radi-nacionalnogo-messengera-max.

180 National Bank of Ukraine, All-Ukrainian information campaign on payment security #ShakhraiGoodbye is launched, 13 May 2025, https://bank.gov.ua/ua/news/all/startuye-vseukrayinska-informatsiyna-kampaniya-z-platijnoyi-bezpeki-shahraygudbay.

181 See https://promo.bank.gov.ua/stopfraud/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net