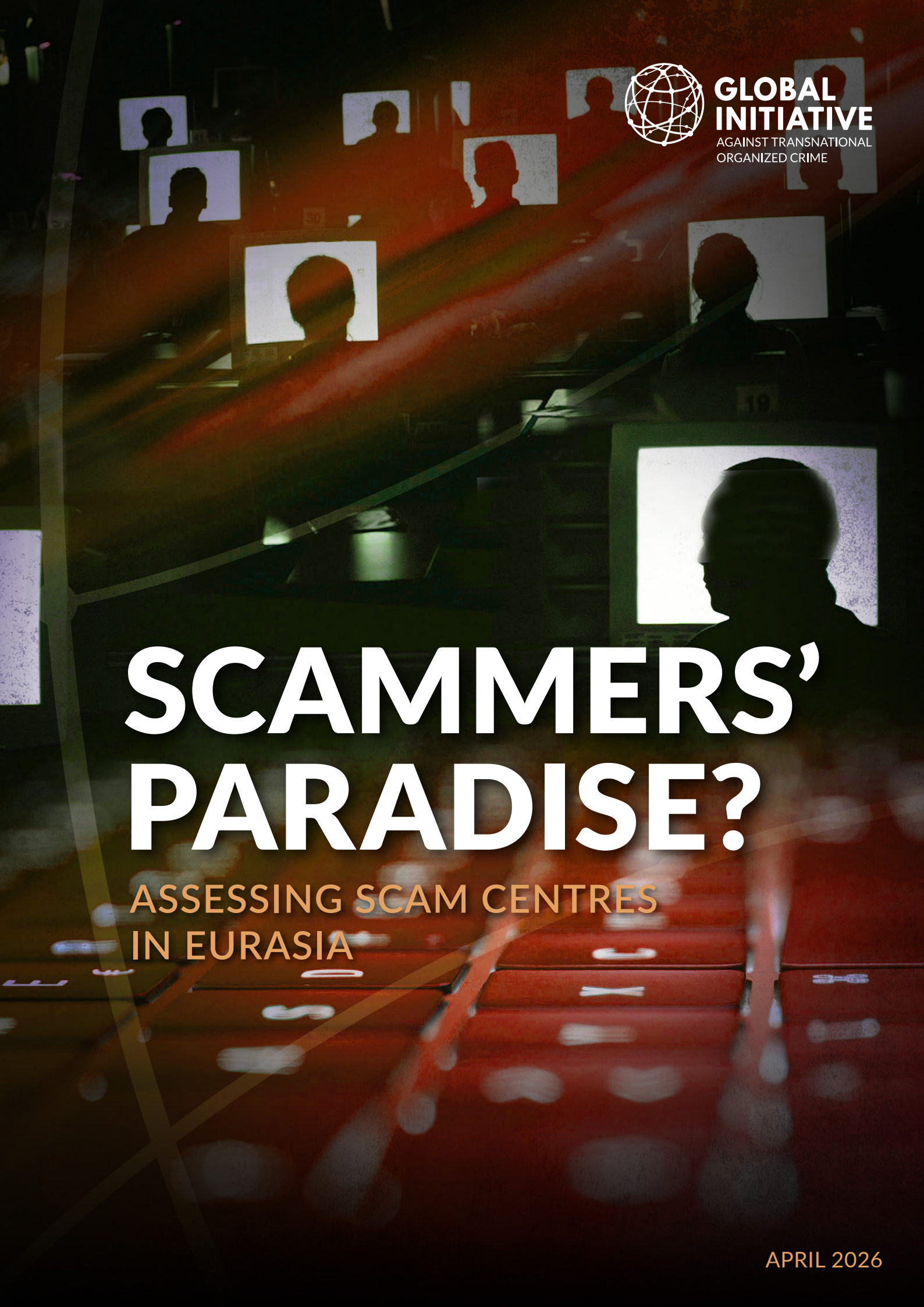


GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

SCAMMERS' PARADISE?

ASSESSING SCAM CENTRES IN EURASIA

APRIL 2026

ACKNOWLEDGEMENTS

The Global Initiative Against Transnational Organized Crime (GI-TOC) would like to thank all those who contributed to this research across the region, especially in Georgia, where our partners and interviewees, who wished to remain anonymous, were very generous with their expertise and experience of the world of scam call centres. We would also like to thank Bektour Iskender, who helped bring insight into dynamics in Central Asia.

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

This research report assesses the phenomenon of scam call centres in Ukraine, Russia, Belarus, Kazakhstan, Kyrgyzstan and Uzbekistan, Georgia and Armenia. Beyond the headline cases exposed by investigative journalists, overall understanding of the operations of scam call centres in this region remains underdeveloped compared to, for instance, South East Asia. This report seeks to provide that coverage.

The central question concerns the extent to which scam call centres operate independently of local factors, given that they target victims around the world using online tools, or if their scope, scale and sophistication are shaped by their location. An ancillary question was to assess the profound political trends that have swept through the region since Russia's full-scale invasion of Ukraine in February 2022 and their effects on this illicit economy, either to its benefit or detriment.

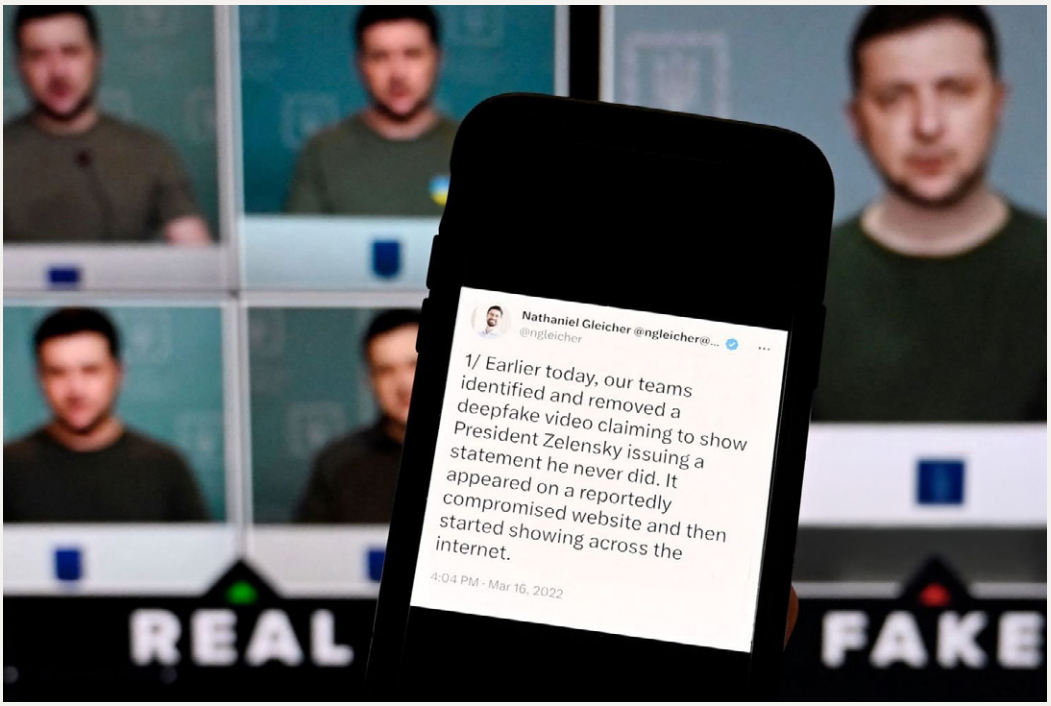
The purpose is to ascertain potential points of leverage for international law enforcement to tackle scam call centres in the region, and to raise awareness of the political, economic and social considerations that may complicate such interventions.

Methodology

Research included fieldwork in Georgia and Armenia in October 2025, along with remote interviews with knowledgeable stakeholders in Kazakhstan, Kyrgyzstan and Uzbekistan, and a comprehensive review of open-source materials in the relevant languages. Research in Georgia was supported by partners with expert knowledge of the scam call centre economy, who produced a detailed analysis of recent cases and current trends. Analysis regarding Ukraine is drawn from interviews and open-source research conducted in early 2025.

The research subject presented several challenges. One was the difficulty of verifying information to prove criminality outside of cases that have gone through court procedures. The scam call centre world is highly secretive and there is often little to distinguish such operations from their legitimate counterparts, except where employees seem to possess unexplained wealth, as evidenced, for example, on social media.[1]

A related constraint was the political factor. In several countries, it is difficult for journalists to report on scam call centres or to cover them beyond the restrictions of state messaging, as in Russia, where scam call centres have become part of the state's propaganda campaign against Ukraine. Interviewees



A fake video shows Ukrainian President Volodymyr Zelensky calling on his soldiers to lay down their weapons. The Russo-Ukrainian war, coupled with the rise of AI-enabled fraud, has multiplied opportunities for online scammers. *© Olivier Douliery/AFP via Getty Images*

who spoke out against call centres must also be understood in terms of their political affiliation, which may make their claims against the government more strident. As one academic, speaking of the situation in Georgia, neatly summarized, 'The entire area of activity is clouded in ambiguity, and its politicization makes it more difficult to untangle.'[2]

Key findings

- **Common toolbox, local variations.** Scam call centres are a regional concern, with most countries seeing a steep increase in activity. All scam centres use fairly similar approaches, using deception and social engineering to extract money or financial information from victims, with local variations in sophistication, scale, staffing and official protection, among other factors. Ukraine, Russia and Georgia appear to be the hotspots for such activity, with Europe and North America the major targets. Within the region, Belarus appears, by one measure, to show the highest exposure to fraudulent activity and Russia appears to be the main regional target for scammers. Armenia, Kazakhstan and Uzbekistan are less active, but show signs of increase.
- **Expanding scam activity underpinned by transnational networks and local enablers.** There is evidence of transnational networks based in and targeting multiple countries in the region. Local enablers provide financial and communication services, such as collecting funds or maintaining SIM boxes that bypass anti-fraud measures. One alarming development is the arrival of East Asian organized crime actors in Georgia, indicating that the region may becoming integrated into global scam dynamics.

- **Scammers exploit geopolitical faultlines.** Recent geopolitical developments have fuelled the growth of the scamming sector. The Russo-Ukrainian war has provided new opportunities for scammers and spurred a surge of 'patriotic' scamming. The war has also accelerated the decline in international law enforcement cooperation between Russia and the West, while Georgia's recent pivot away from the EU has reduced the influence of Western partners in the country. Within Eurasia itself, regional cooperation is defined by the state of relations with Moscow and other external partners – Belarus, Kyrgyzstan and Kazakhstan have all enhanced cooperation with Russia as part of a broad pushback against scammers, while Ukraine and Russia have zero cooperation. Overall, the geopolitical divisions between Russia and the West, and within Eurasia itself, has created the perfect conditions for scammers to operate – a scammer's paradise.
- **Criminal benefits of authoritarian practices and corruption.** Official actors play a significant role in shaping both the understanding and protection of the scam call centre economy – two often interlinked aspects. In countries such as Russia and Belarus, where there are strong restrictions on independent investigative journalism, much remains uncertain about the structure of the scam call centre ecosystem, particularly in regard to official protection. In Georgia, where corrupt state actors play a key role in scam centres, the space for investigative journalism is rapidly shrinking as the country pursues a more authoritarian path. By contrast, Ukraine's media continues to be active in exposing the activities and organization of scam centres.
- **From AI-enabled human scams to human-enabled AI scams?** Scam call centres have grown more sophisticated. Today, deepfakes, voice cloning, instant document translation and image generation, among other tools, provide scammers with an arsenal that grants them much greater reach and extremely high levels of plausibility for deception. If this trajectory continues, the balance may soon switch from AI helping human scammers to humans facilitating AI-led scams.

INTRODUCTION: HOMEGROWN AND IMPORTED

Scam call centres have become global news in recent years, but it is the model that developed in South East Asia that has garnered most of the coverage: large compounds in shady borderlands, often using internationally trafficked workers.[3] This is not to say that Eurasia has been neglected. Investigative journalists have done much to expose the scale and sophistication of scam call centres in Georgia, Ukraine and elsewhere,[4] but an overall assessment of the scam call centre ecosystem in the region has arguably been lacking.[5]

The need for such an assessment is clear from current research that often emphasizes the spread of a South East Asian 'business model' around the globe, especially in terms of human trafficking.[6] This approach risks overlooking the extent to which the Eurasian region has developed its own distinctive traits in the practice of scamming. Even within the region, there are notable variations – in scale, sophistication, treatment of workers and political climate – that must be considered, especially in the wake of Russia's full-scale invasion of Ukraine.

In short, scam call centres in Eurasia are a diverse phenomenon that must be understood on its own terms, although the recent entrance of East Asian criminal actors to Georgia, and the alleged involvement of one Eurasian transnational crime group in Myanmar, suggests that Eurasia may be integrating into the larger global scam picture.[7]

Scam call centres are a relatively recent criminal innovation in Eurasia. Telephone-based fraud has been around for decades, but the innovation of call centres – large operations using Voice over Internet Protocol (VoIP) and other technologies in a variety of sophisticated schemes to target victims across the globe – appears to have taken place in the 2010s and underwent rapid acceleration.

One early vector of this appears to be the emergence of so-called 'binary options' in Israel in the mid-2000s, which were essentially fraudulent investment schemes based on speculation on the price of an asset.[8] The size of this industry was vast, with one estimate alleging a total market revenue of US$5–US$10 billion a year.[9] Many of the companies involved in binary options took advantage of a gap in Israeli legislation under which the authorities did not scrutinize firms that only targeted customers overseas.[10]

Things began to change when Israel passed legislation in 2017 banning the overseas sale of binary options, which apparently drove some Israel-based operations to migrate to Eurasia. The Milton Group, reportedly formed in Israel by Georgian-Israeli nationals, was one such case.[11] The group moved to Ukraine and Georgia (under the Morgan Group brand) around or after in 2016, sometime after a *Times of Israel* report exposed the issue of binary options and the topic began receiving widespread attention in Israel.[12] The same newspaper characterized the Milton Group's operations as 'the latest mutation of Israel's binary options industry'.[13] A Georgian journalist described the business as being 'copy-pasted into Georgia'.[14] In May 2024, the head of the Milton Group was extradited from Armenia and the Bavarian Cybercrime Unit formally filed charges over alleged fraud that resulted in estimated global losses of at least €180 million. In February 2026, he was sentenced to seven and a half years in jail for his role in the scam.[15]

The Milton Group is not the sole instance of Israeli actors in Eurasian scam call centres. Envirotech, linked to the GetFinancial Group, whose leaders pleaded guilty to fraud estimated at €77 million in 2023,[16] was reportedly founded in Israel in 2014 and opened its first call centre in Tbilisi in 2016. The Israeli side of the operation was liquidated in 2017, around the same time as the legislation banning binary options was approved,[17] but the group continued to expand, opening call centres in Moldova and Armenia in 2018.[18] Israelis in prominent managerial roles have also been linked to scam call centres in Serbia, Bulgaria, Spain and Cyprus.[19]

This ability to translocate may be one of the most distinctive facets of the call centre economy. Relocating often poses serious challenges for organized crime,[20] but scammers seem to find few problems in setting up shop somewhere new. This may reflect the corporate, as opposed to criminal, structure of scam call centres. Managers of the enterprise may belong to a criminal network, but the superficial resemblance to licit employment for the workers – regular salary, perks, a stable place of work – lessens the need for criminal secrecy and culture.

Of course, Israeli and dual-national citizens were not solely responsible for the acceleration of scam call centres in Eurasia. Different models were simultaneously forming elsewhere in the region of their own accord, but the sophisticated practices of these Israeli-origin operations may have provided a potent proof of concept that was soon adopted and improved upon.

Rising rates of internet access also provided the necessary infrastructure for scammers in the region. Eurasia was coming online, and scam centres were a potent way for criminals to access a new global market. In Georgia alone, the population share of internet users almost tripled between 2010 and 2020, from 26.9% to 72.5% (Figure 1). The business environment also presented few obstacles. In Georgia, for instance, opening a bank account is very easy, and one can register a company in a single day.[21] A limited liability company can also be registered in one day in Ukraine, although the preliminary process is more convoluted.[22] By the early 2020s, scam centres were a fixture in three Eurasian hubs: Georgia, Ukraine and Russia.

In Georgia, the Black Rock call centre – identified by a whistle-blower as engaged in criminal activity[23] and the subject of investigations and asset freezes by the prosecutor's office[24] – was registered in June 2020.[25] The AK Group – which allegedly stole more than US$35 million between May 2022 and February 2025, according to its own financial records[26] – was registered in April 2021. In March 2025, after an OCCRP investigation and report,[27] the Georgian prosecutor's office launched a criminal investigation into possible fraud and money laundering by the AK Group, but there has been no further comment on the case at the time of writing.[28]

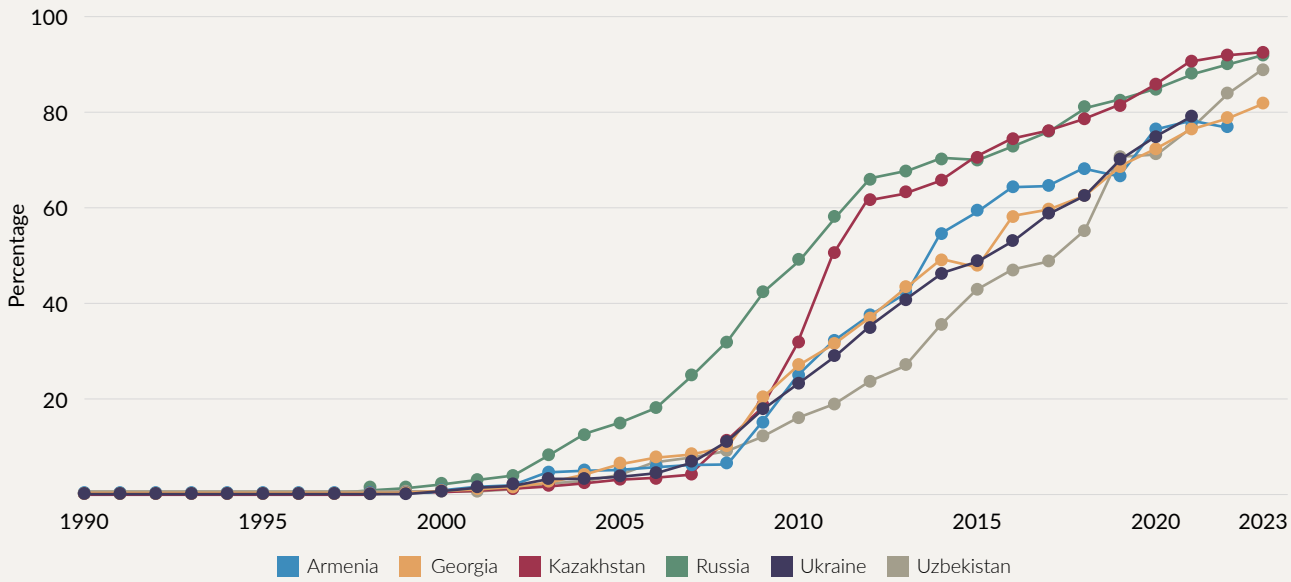


FIGURE 1 Share of population using the internet in selected countries, 1990–2025.

SOURCE: International Telecommunication Union

In Ukraine, the number of scam call centres proliferated, reaching an estimated peak of between 1 000 and 2 000 in mid-2023 before a crackdown reduced their number.[29] Russia also showed notable increases in activity as scam call centres migrated from the penitentiary system into regular society.

The call centres all utilized a range of scams, mainly imposter scams or sophisticated investment scams involving cryptocurrency, complete with 'live' trading platforms. But as the following sections will show, there were also significant variations in how these operations were structured and their modalities, many of which were due to the specific local contexts and prevailing political climate.

REGIONAL COMMONALTIES, LOCAL VARIATION

The scope and characteristics of scam call centre activity vary considerably across Ukraine and Russia, Kazakhstan, Kyrgyzstan and Uzbekistan, as well as Armenia and Georgia, reflecting their distinct national conditions. Nevertheless, clear patterns and similarities can be observed throughout the region.

One of the most notable findings was how rapidly and widely scamming has spread across the region[30] – and how sophisticated and damaging it has become. A diverse ecosystem operates in the region, and each location blends commonalities with its own characteristics. In terms of market activity, for example, Georgia does not host nearly as many scam call centres as Ukraine or, probably, Russia, but its groups are notable for their reach, sophistication and losses incurred.

Another illuminating metric is market consolidation: whether most scam call centres belong to networks or operate individually. Ukraine shows evidence of a high level of consolidation, with most scam call centres run by a handful of criminal networks. In Georgia, the market may be considered highly consolidated, given allegations of control by the governing party, but it is also apparently a free market where entrepreneurial call centres can set up without having to belong to a larger criminal network.

European and other Western countries remain major markets for victim targeting, due to their comparative wealth, but scammers also operate widely in the region, benefiting from the fact that Russian remains a common language.[31] Scams in Kyrgyzstan and Uzbekistan, for instance, are carried out mainly in Russian. During fieldwork in Armenia, the GI-TOC heard that many scams there were conducted in Russian.

More sophisticated operations may abide by a 'don't work where you live' rule or refrain from targeting citizens of the country where the scam call centre is based.[32] Some scam call centres were said to calibrate their operations according to the risk of law enforcement exposure. In Georgia, for example, interviewees said that scammers would not target people in Germany and the US, which are considered the most active in pursuing fraud cases. Given the lucrative nature of these markets, though, the extent to which this is applied is doubtful.

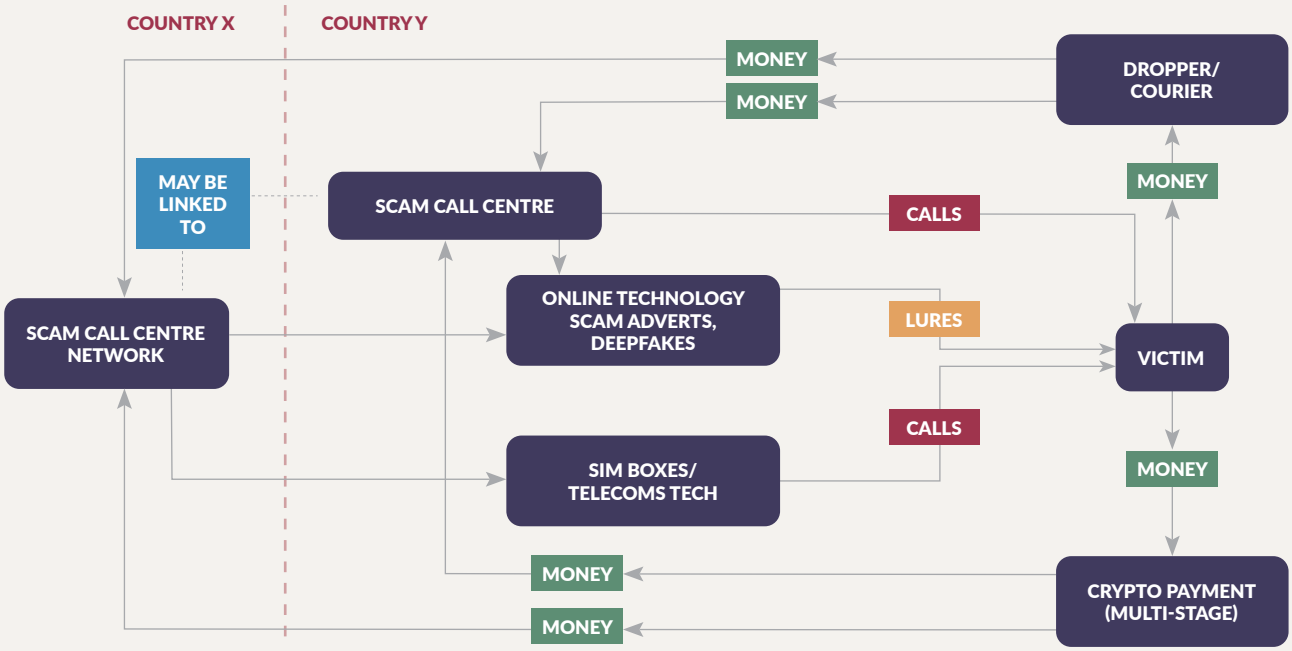


FIGURE 2 The regional architecture of scam call centres in Eurasia.

Geographically, Georgia, Ukraine, Russia and Belarus appear to have the greatest presence of scam call centres, with Armenia, Uzbekistan, Kyrgyzstan and Kazakhstan primarily serving as target countries rather than hubs of scam activity on their own right. However, the latter countries also show evidence of an increase in scamming activity, sometimes with the involvement of transnational networks. Russia appears to be the primary target of scammers, perhaps as a reflection of its high GDP.

Finally, it is clear that, while the telephone remains a major tool for socially engineered scams, it is by no means the only one. Scammers are increasingly adopting hybrid approaches that may also include messages, malware, phishing and artificial intelligence. Indeed, AI researchers have already created large-language-model scam agents that can make successful scam calls for as little as a dollar – a fact that could radically reshape the nature of the market.[33] The next generation of the scam call centre in Eurasia may look very different to the current incarnation, moving towards human-enabled AI scams, as opposed to the other way round.

The scam toolbox

Most scam call centres rely on a common box of tricks that use social engineering to a greater or lesser extent. Higher levels of social engineering are associated with high-value scams like investment or romance scams, where a victim is cultivated over time and persuaded to part with significant sums of money. High-volume low-value scams, such as offering fake goods, may generate lower returns but can be largely automated and widely scaled.

Fake goods scams: Goods are advertised on social media and websites to attract victims who pay but never receive the goods. There are many variations. Sometimes the fraudster demands a pre-payment to cover customs or other fees. In 'lottery' frauds, victims are convinced to pay an advance fee to receive a large cash reward. They generally involve low levels of social engineering.

Imposter scams: These take the form of a call from a state official, law enforcement officer, bank employee or anyone with status. Such frauds often create a climate of urgency where the victim is told to transfer money to avoid prosecution or even, ironically, fraud.

Investment scams: One of the most sophisticated fraud types, investment fraud identifies victims with significant assets and, sometimes, a predilection to invest. Over time, the scammer persuades a victim to transfer money, sometimes using deepfakes of celebrities as a lure and fake trading platforms where victims watch their 'investment' increase.

Romance scams: The scammer cultivates a romantic connection with a victim before gradually introducing the notion of transferring money, perhaps to buy a property together, facilitate travel or help them out of an emergency scenario.

Ukraine: a booming wartime illicit market

Reports of the Milton Group's operations in Kyiv first brought scam call centres to public notice, but the market in Ukraine has now become much more widespread and active. The period after the Russian invasion of February 2022 appears to have seen a rapid increase in the number of scam centres, in part fuelled by the surge of 'patriotic' scamming as Ukrainians targeted Russian victims. From their traditional hubs in Dnipro and Kyiv, call centres have now been reported in all regions of Ukraine, including the occupied territories. They have become one of the most lucrative criminal activities in Ukraine, earning an estimated US$1 billion per month.[34]

According to GI-TOC research, the market is highly consolidated, with most call centres belonging to several networks, or 'grids', managed by organized crime actors.[35] Young adults are recruited to work in scam call centres with promises of high salaries, only to find that the basic wage – without the enticing but hard-to-reach bonuses – is far less impressive. Many of them leave. Successful scammers find it much more difficult to quit, with scam centre bosses applying pressure and threats to make them stay.

Estimates of the number of scam centres operating in 2023 ranged from 1 000 to 2 000, although this number fell after a series of crackdowns, perhaps by as much as a third. In 2025, a new wave of crackdowns under the new prosecutor general saw hundreds more shut down. This may signal a turn in the fortunes for the market, but it is complicated by the level of corrupt official protection granted to the scam call centres.[36] Some raids in the past have turned out to be purely cosmetic. It is also possible that the scam centres that were shut down lacked the necessary protection (or 'roof'), while others with the right cover continue to work as before. It therefore remains to be seen whether the tide has genuinely turned.

Russia: the fog of war

Since the war began, it has been difficult to get a sense of the scale of scam centres operating within Russia, given that Russian (or Russian state) media reports claim that almost all telephone scams in Russia are remotely launched from Ukraine.[37] In this formulation, Russians emerge as the victims of external scammers, not the perpetrators. Even when scam call centres in Russia have been raided, the media are quick to suggest the role of Ukrainian handlers.[38]

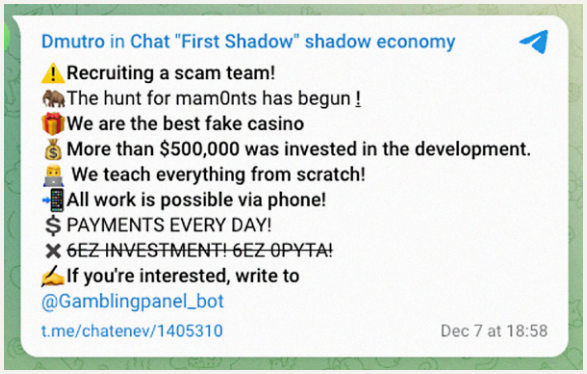
For example, media reports on the December 2024 bust of a Moscow call centre that was allegedly connected to the Milton Group claimed that the stolen funds were used to finance the Ukrainian Armed Forces: 'The criminal network allegedly operated under the control of the leader of the Khimprom organized crime group, with patrons and handlers within the Security Service of Ukraine.'[39] Russian outlets were also quick to seize on the theory that Valeria Fedyakina, a Russian scammer known as 'Bitmama' who was convicted for a €20 million bitcoin fraud, donated part of the proceeds to the Ukrainian Armed Forces, despite the fact that this information did not appear in the official charges.[40] One Russian police official even alleged that some Ukrainian scammers are employed by the economic crimes department of the Odesa region or the criminal investigation department of the Dnipropetrovsk region.[41]

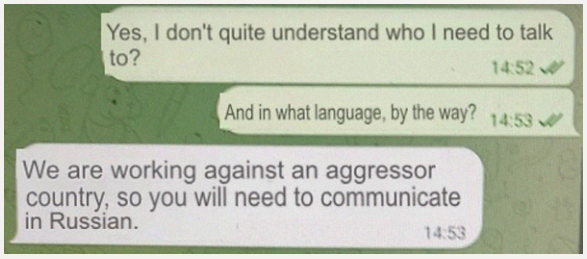
Khimprom, the enemy's criminal

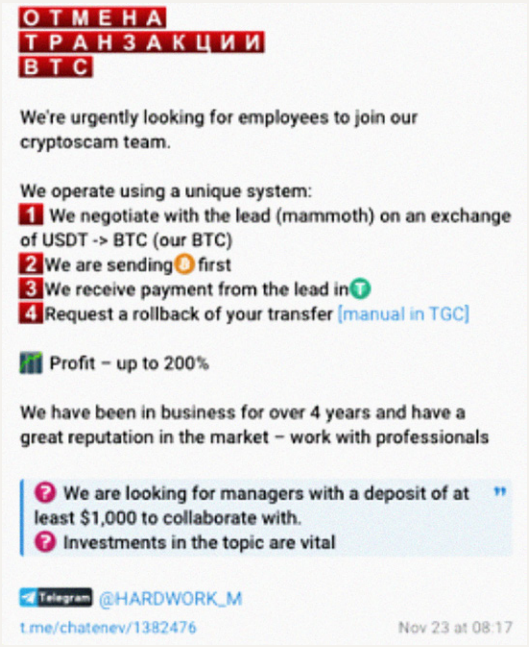
The organized crime group Khimprom has long been a political football between Russia and Ukraine. Each side claims that Khimprom operates at the behest of the other, especially in drug trafficking.[42] The origins and political affiliation of the group have been the subject of heated debate, but it has operated in the illicit synthetic drugs trade in both Ukraine and Russia for years,[43] before expanding to scam call centres in Ukraine, Russia and, by one account, South East Asia.[44] The alleged presence of Khimprom in Kazakhstan, where it is reportedly engaged in synthetic drug production, also raises concerns that it will operate call centres there.[45]

While it is true that Russia has become a major target for Ukrainian scammers, the lack of independent media reporting obscures the presence of a significant domestic market. Some indication of the domestic trajectory of socially engineered scams in Russia can be gleaned from pre-2022 reporting that shows a flourishing scamming ecosystem. Scam call centres in Russia reportedly emerged in the prison systems in the mid-2010s and quickly proliferated, with hundreds of 'black' call centres operating with the collusion of prison officials.[46] These soon began to spread beyond the prisons, reportedly protected by local law enforcement.[47]

Statistics show a steep rise in scamming attacks. According to Sberbank, mobile phone fraud surged by 91% from 2018 to 2019, including attacks from both inside and outside the country.[48] Russian scammers also benefited when the coronavirus pandemic pushed more people online.[49] Today, socially engineered forms of scamming are pervasive in Russia, enabled by rising levels of leaked data that give scammers the material to tailor their attacks.[50] The prosecutor general estimated that social engineering accounts for two-thirds of all phone and internet fraud.[51] Fake bank and state agency calls and investment scams were the most prominent tactics in 2025.[52]







Adverts for Russian call centres on Telegram and a text exchange with Ukrainian call centre recruiter openly discussing scamming Russians.

It appears that some scam call centres in Russia have assumed a similar form to the model developing in Ukraine.[53] A former employee recounted working for a scam call centre in the heart of Moscow that operated relatively openly, albeit with high security, mirroring the trend in Kyiv and Dnipro for scammers to rent office space in centrally located business centres.[54] The former scammer stated that monthly salaries typically ranged from US$950 to US$2 100, but they could gain the same amount in bonuses from closed deals, and the most proficient could earn much more. Still, working in this call centre would not have been lucrative in a lean month, considering the average salary in Moscow in 2025 was US$2 000.[55]

Russian call centres, like their Ukrainian counterparts, advertise openly for workers on Telegram, and even use similar terms, such as 'mammoth' for victims. That said, it was apparently far easier to engage with Ukrainian than Russian scam call centres. One investigative journalist, who had attempted to be hired by operations in Ukraine and Russia, described Russian scam centres as 'impenetrable fortresses for random outsiders – you really need to reach the state of one-on-one interviews to make them reveal what they actually do'.[56]

Droppers under pressure

'Droppers' are a key feature of the money laundering architecture that scammers use to receive and move illicit gains. In essence, they are third parties whose bank accounts are used by scammers as illicit finance nodes. Some droppers may not realize that they are being used for crime, but others do and may have dozens or even hundreds of accounts, receiving a cut for their trouble. The scale of their activity is massive: in 2025, more than 2 million people were said to be involved in cashing out scams, a number that included both droppers and their 'curators' (the scammers directing them).[57] In 2024, approximately 10 million Russian bank clients transferred money to dropper accounts.[58] The profile of a dropper is broad, but marginalized and young people are often used, with little understanding of the risks they run.[59] Approximately half of the droppers in Russia are under the age of 23.[60]

Russia, Uzbekistan and Kazakhstan all passed laws to inhibit droppers in 2025.[61] According to the Bank of Russia, these measures have already had significant results. Dropper

transactions decreased threefold between 2024 and 2025, while the average transaction size decreased tenfold.[62] Telegram advertisements offering accounts had also decreased. Scammers have since changed to using accounts opened by legal entities, although this tactic is also coming under pressure.[63]

At the same time, there are indications that scammers are looking for other ways to evade digital traces. The Russian Cyber Police Telegram account,[64] for example, reported that scammers have moved from having victims make a direct transfer to persuading them to buy gold, sell it at another bank and transfer the amount.[65]

Couriers, often recruited through Telegram,[66] are also used to collect cash and assets such as gold in person, replicating a tactic used by scammers in Germany and elsewhere. In one illuminating case, a man from Novosibirsk travelled 4 000 kilometres to collect 2.32 million roubles (US$30 000) from a victim in Saint Petersburg. The scammers paid for his travel and hotel and told him to buy a white shirt, trousers and shoes to 'look respectable'. His fee for the job was 2% of the take – approximately US$600. He was later identified and arrested for fraud.[67] ■

A recent trend in Russia is the emergence of hybrid scams that combine different methods. Forms of social engineering may be used with malware tools disguised as legitimate software, such as an app that allows the scammer to make a virtual copy of a bank card.[68] Crypto–romance scams combine romance and 'pig butchering' investment fraud.[69] In romance–delivery scams, the victim is drawn into a relationship and then asked to pay for delivery of a fictitious expensive gift or cinema tickets.[70]

AI is also fuelling romance scams and personalized phishing attacks – effectively an AI-automated form of spear phishing – with the volume of such emails increasing by 53% between January and August 2025.[71] In the future, according to one Russian analysis, 'attackers will increasingly use artificial intelligence to create personalized emails and deepfakes, enhancing the effect of psychological pressure.'[72]

Scammers also use tech to reach victims. There have, for instance, been cases of children being targeted through video games, echoing a trend seen elsewhere in the world.[73] The Telegram platform is also used to attract young jobseekers. The page advertises an easy, well-paid job, but when someone responds, the vacancy has closed. They are then offered opportunities in investment schemes, before being directed to a phishing website or perhaps their phone number is passed to a scam call centre.

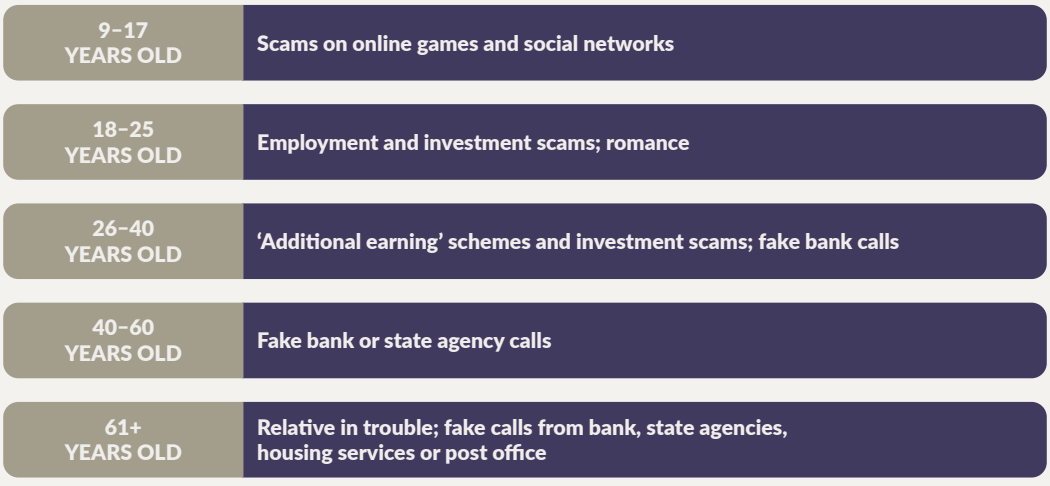
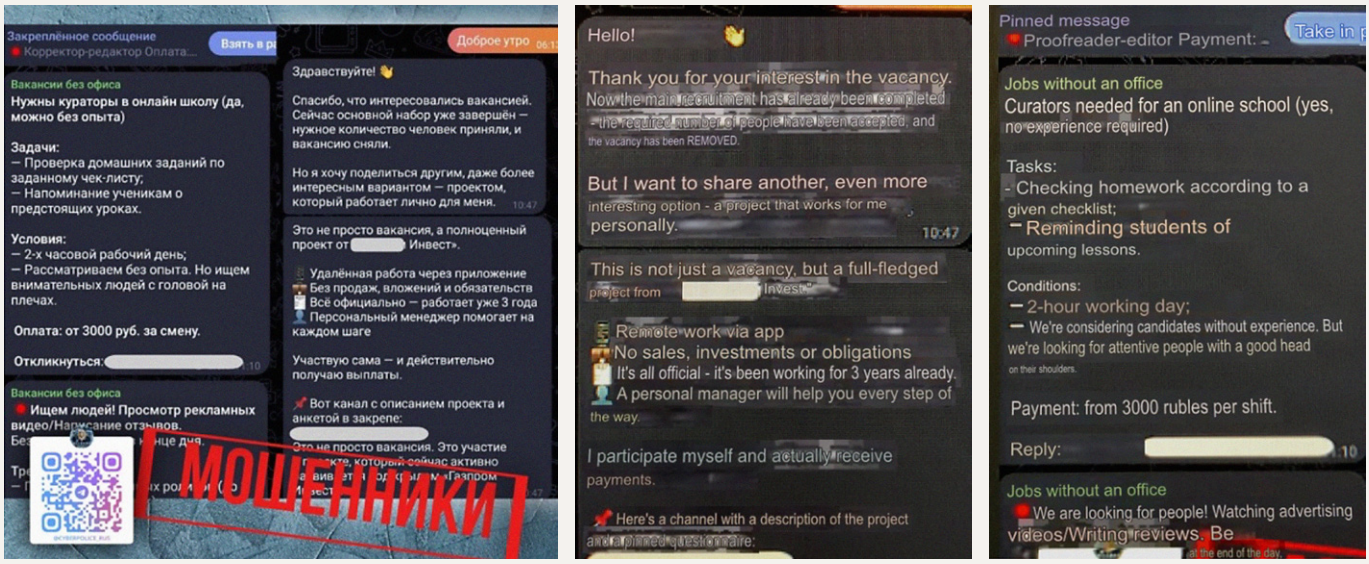


FIGURE 3 Common scams in Russia by victim age groups.

SOURCE: Bulletin of the Russian Cyber Police, Telegram, 23 November 2025, https://t.me/cyberpolice_rus/4397



An investment fraud scam on Telegram. *Photos: Bulletin of the Russian Cyber Police, Telegram, 19 May 2025, https://t.me/cyberpolice_rus/3648*

According to one analyst, Russia is the main target of scammers based in former Soviet republics,[74] and it is clear that Russians are losing serious money to socially engineered scams. The Federal Security Service (FSB) stated that 640 000 cases of remote fraud were reported in 2024, with losses exceeding US$2.1 billion.[75] The Sberbank financial services company estimated 2024's losses even higher, at approximately US$3.2 billion.[76]

Russia has made various efforts to crack down on the scammers, including by targeting 'spoofing' – a practice in which scammers can masquerade as calling from within Russia – but there are mixed signals regarding the efficacy of these efforts. Sberbank found that the daily number of scam calls in 2025 had decreased to 5–6 million, down from 8–10 million in 2024.[77] However, the amount of funds stolen continues to rise and schemes are becoming ever more sophisticated. In October 2025, a police official said that about 80% of all cybercrime reports in Moscow, including scams, were for damages above 250 000 roubles (US$3 000), with damages of 1 million roubles (US$12 250) becoming commonplace.[78]

Foreign-based scammers also engage in 'spoofing', a practice that allows them to masquerade as calling from within Russia. The state has made various efforts to crack down, but the rising use of SIM boxes – which allow an internet link to local SIM cards – has proven an effective workaround for scammers. There are Russian media reports of scammers from Ukraine and other unidentified countries using Russian locals as enablers, including through the provision of financial and communications services[79] and, possibly, money laundering nodes.[80]

Belarus: most exposed?

Belarus is keen to project the image that it is getting to grips with its rising tide of fraud.[81] Special cybercrime law enforcement departments have been established within the national investigative committee and the ministry of internal affairs.[82] Belarus has also expanded its cooperation with partners in the region to tackle scam centres.[83]

According to the Ministry of Internal Affairs, such efforts appear to be paying off, with 2025 a tipping point: for the first time in recent years, the number of cybercrimes reportedly decreased, down 11% for the first 10 months of 2025 compared to the same period in 2024, with frauds down by almost 20%.[84] During roughly the same period, 31 200 fraud attempts were prevented.[85]

However, such figures should be taken with caution, given the political manipulation of crime statistics and the lack of independent verification or corroboration.[86] Other figures paint a more sobering picture. Belarus's overall reported losses due to fraudulent card transactions[87] – 18 million Belarusian rubles (approximately US$6.2 million) in Q3 of 2025[88] – may be relatively low compared to Russia and Ukraine, but some of the individual reported cases have seen huge losses. Every one of top 10 scams of recent years listed by a local media outlet saw Belarusian citizens suffer losses in the hundreds of thousands of dollars.[89] And even the overall numbers become concerning when factoring in Belarus's relatively small population of fewer than 10 million inhabitants. Indeed, on a per capita basis, Belarusians may be one of the most exposed nationalities in the region when it comes to fraud (Figure 4).[90]

The flurry of recent takedowns also illustrates the extent to which Belarus has developed into a base for scam call centres, some of them sizeable, sophisticated and transnationally linked.[91] A scam call centre shut down in mid-2025, for example, advertised jobs on foreign employment sites and then provided 'training' to applicants before giving them opportunities to work as brokers – a convoluted lead-up to an investment scam.[92] AI has also been increasingly used in scams in Belarus.[93]

The busts also showed that increased cooperation between Belarus, Russia, Kazakhstan, Kyrgyzstan and Uzbekistan may be paying dividends, enabling authorities to coordinate operations against all the nodes of transnational networks. But an important caveat must be applied. As in Russia, the media in Belarus is highly restrictive, making it difficult to gather information beyond official pronouncements that also often blame Ukrainian scammers. While state-directed media and ministry officials may well be trumpeting their successes, it is impossible to know whether their efforts are seriously undermining the current ecosystem or merely targeting a few prominent actors. Independent media in exile that retain contacts and networks within the country, such as BelPol, may be able to shed greater light in the future.

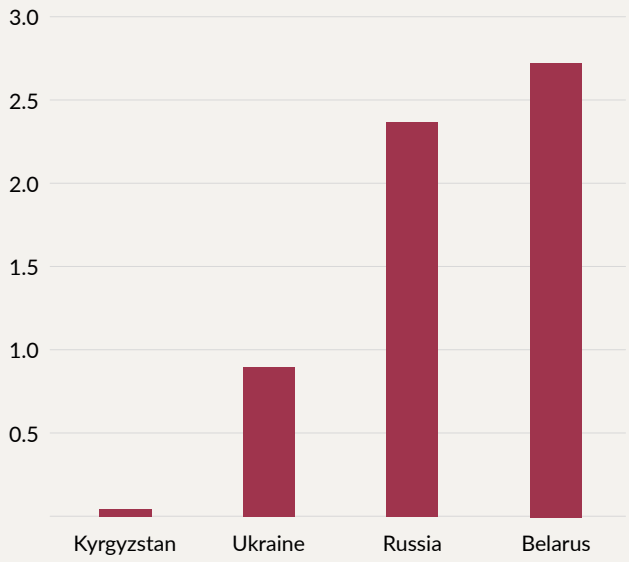


FIGURE 4 Comparative risk exposure to fraud, by fraudulent card transactions per capita (US$).

NOTE: 2024 annual data used for Russia and Ukraine; Belarus figure extrapolated from losses reported for Q3 2025; Kyrgyzstan figure extrapolated from Q1 and Q2 2024 reports.

SOURCE: Data from local media sources[94]

Kazakhstan, Uzbekistan and Kyrgyzstan: targeted from abroad

The scam call centre picture for Kazakhstan, Uzbekistan and Kyrgyzstan is somewhat obscure, although they all face rising levels of scam activity.[95]

There is little evidence of a strong domestic scamming industry in any of the three countries, although pockets of sophisticated domestic scamming do exist. In 2025, only two scam call centres were shut down in Kazakhstan's capital, Astana, one of which notably targeted fellow Kazakhstanis.[96] A case in the Akmola region saw scammers steal 102 million tenge (US$200 000) from a Bulgarian citizen.[97] In Kyrgyzstan, there are signs of a transnational footprint: a Belarusian citizen arrested in Bishkek in June 2024 for running a fake investment scam was allegedly part of a wider fraud network with branches in Belarus and Russia.[98] In Uzbekistan, four call centres run by two different groups were shut down in the space of a month in early 2025.[99]

Instead, most scams targeting citizens in Kazakhstan, Uzbekistan and Kyrgyzstan appear to be launched from elsewhere and often conducted in Russian, suggesting origins in other Commonwealth of Independent States countries.[100] A Kyrgyz journalist, citing sources in law enforcement, spoke of Russian and Belarusian scammers particularly targeting Kyrgyzstan.[101] Scammers targeting Kazakhstan have been traced to Ukraine and other member countries of the Commonwealth of Independent States.[102]

Explaining this situation, a Kazakh lawyer who works in the field commented that 'it would be very stupid to [deceive] people who are in the same country. Usually, scammers are transnational. It is better and safer for them to do it because of the border.'[103] But that does not mean locals are not involved. As in Russia, local droppers and SIM box providers offer operational services to scammers located abroad.[104] Locals are paid 20 000–30 000 tenge (US$50–US$60) per month to keep the SIM boxes that enable foreign scammers to dial in with local numbers.[105]

In terms of volume, Kazakhstan appears to be a major target for phone fraudsters. Official statistics show that 67 million scam phone calls were blocked there in the first nine months of 2025.[106] Uzbekistan's statistical picture is complex. The country, for example, has apparently had a dramatic reduction in impersonator scams. After the COVID-19 pandemic, with more people online, there was a boom in bank-employee impersonation,[107] with law enforcement impersonation emerging in 2024.[108] By one reckoning, it accounted for 95% of fraud, but has since dropped to 12%–13%.[109] In the city of Tashkent, impersonator scams accounted for 3.2% of all cybercrimes, affecting 300 victims in 2024.[110] However, other measures point to a booming online scam landscape: in the first 11 months of 2025, the Ministry of Internal Affairs estimated that approximately US$154.9 million had been lost to cybercrime, almost all of which is related to bank card fraud.[111] Kyrgyzstan's losses are more modest, with some US$7 million lost to online fraud in 2025, albeit with a population a fifth of the size of Uzbekistan's.[112]

Playing on paranoia in Kyrgyztan

A common scam in Kyrgyzstan plays on citizens' fear of state authorities, which has intensified since the current government came to power in 2021 and ramped up repression. Among older victims, memories of Soviet surveillance may also loom large.[113] In a common version of the scam, one caller pretends to be an officer of the national security agency and intimidates the victim with invented charges. Another caller presents himself as representing the national bank and offers to help. Sometimes a third person acts as an intermediary who claims to settle the issue.

A journalist who has researched this extensively in Kyrgyzstan gave the following description:

> The person they impersonate is someone important and authoritative [in your organization] but someone you do not have close access to, like a university rector. The scammers put up a profile picture of that person, introduce themselves and say something like: 'You know, your colleague is suspected of some transnational crime. Did you notice any suspicious behaviour? I am just asking because the GKNB [Kyrgyzstan's national intelligence agency] were interested in her.'
>
> A couple of days later, they escalate. They say, 'Representatives from the GKNB came to us. You are also under suspicion. You need to act urgently. I am very concerned about you and have arranged everything. They will call you from the GKNB.' People start receiving calls from the GKNB, the national bank or another agency. The person pretending to be from the intelligence services intimidates the target, saying there is a criminal case against them. Another person reassures them, saying, 'Do not worry, we are resolving everything. We are handling it.' The national bank calls, saying that their accounts may have been accessed by scammers and now they need protection. To get that protection, the victim is told to withdraw money from their accounts and transfer it to another account, which they provide.

Victims are instructed to transfer money to supposedly safe accounts that are actually controlled by the scammers. Losses can be substantial. In one case documented by the journalist, a woman sold her apartment and transferred US$76 000 to the scammers.[114] ■

While scam centres may not be heavily present domestically, it appears that there is a flourishing scam landscape on social media, though whether this is foreign-based or local is difficult to determine. Scammers are taking advantage of the dramatic rise in smartphone adoption and cashless payments in the region (particularly in Kazakhstan),[115] with Telegram the primary source of news.[116] In Uzbekistan for instance, reporting on scams repeatedly highlights the prevalence and variety of scams on Telegram, including malware, [117] fake prizes,[118] pyramid schemes[119] and 'triangle' crypto scams[120] – alongside 'aspirational' scams involving work placement abroad, cars and housing.[121] This is not to suggest that scam call centres are not a real issue in the region – Kazakhstan remains a major target, and Uzbekistan also shows worrying trends – but that they exist in a diverse landscape where complex scams on social media are becoming more prevalent.

Another possible trend to watch for is scammers taking advantage of countries without stringent regulation of SIM card purchases and droppers to become supplier hubs for other countries in the region. In February 2026, for example, a Kyrgyz group was arrested for selling activated SIM cards and dropper accounts on Telegram to international scammers who then posed as state officials to accuse people of terrorism to extort money – a common scam in the country, as described above.[122]

Georgia: a regional anomaly

With only 3 million people, Georgia is one of the smallest countries in the region, but its scam operations are highly developed. As mentioned above, this may be due to the influence of the original Israeli model of

the Milton Group, but even so, it is a more limited market. Most call centres are concentrated in Tbilisi, with interviewees suggesting that there may be a few in Batumi as well. In Tbilisi, estimates varied. One investigative journalist stated that there were 'hundreds' in the city, while a lawyer said that there were between 50 and 100, and mostly small, staffed by only 5 to 10 people, with 50 considered a large call centre.[123] In comparison, a large call centre in Ukraine has as many as 250–300 employees.[124]

In terms of targeting, Georgian scammers adhered to a self-imposed rule to not target their compatriots.[125] This rule may even apply to scam call centres in other countries that are affiliated to a Georgian branch: a Russian former scammer who indirectly stated that he had worked for a Georgian-linked group said that there was one rule: 'not to deceive citizens of the country in which the call centre is located'.[126] During fieldwork in Tbilisi, interviewees suggested that the taboo on scamming fellow Georgians was entirely pragmatic – Georgian victims do not have much money, and it was relatively easy to track down scammers who spoke Georgian.

Two of the largest operations in Georgia, Morgan Limited and AK Group, also had a prohibition on targeting the US, according to investigative journalists.[127] It was unclear why, but the long reach of the US – one of the few states with the resources to track convoluted illicit financial flows across financial systems and blockchains – may be a factor.[128] Scammers were also reportedly wary of targeting Germans after German law enforcement sent their own team of investigators to handle a case in Tbilisi.[129] 'They came to Georgia several times,' said a Georgian investigative NGO member. 'All the joint special operation work was done by the Germans. They sealed all the equipment and interrogated the suspects.'[130] A cyber expert stated that there is also a compelling diplomatic reason why Georgian law enforcement cooperated with the US and Germany: blocking or ignoring them completely would risk a deterioration in relationships at higher political levels.[131]

Morgan Limited: A Georgian scam powerhouse

Various sources, including the company's own lawyer,[132] claimed that Morgan Limited was one of the largest scam call centres in Georgia. Founded in Tbilisi in October 2018, it was owned by a Ukrainian woman who served only a nominal role and was connected to the Milton Group in Ukraine.[133]

Morgan Limited established a call centre at Otar Chkheidze 10 in central Tbilisi and set about hiring German-, English- and Russian-speaking agents and managers, as well as creating various fake trading platforms. 'Clients' – mainly from Europe – were encouraged to register on these platforms and associated crypto exchanges. The victims' funds were transferred to foreign bank accounts and crypto wallets controlled by the criminal organization. At the same time, the platforms showed victims an increase in the invested funds through simulated actions. If the victims demanded the return of these funds, all communication was terminated.

Between 2019 and 2021, an official investigation established that Morgan Limited illegally appropriated a total of €5 053 072 from the identified victims, who were citizens of Germany, Slovenia and Slovakia. The largest single loss was suffered by a German citizen who transferred €2 079 607 to Morgan Limited. However, the crime extended beyond these three countries, and the total amount extorted is likely to be much higher than the investigation was able to detect.

On 27 June 2025, the Georgian prosecutor's office reached a plea agreement with the defendants, imposing only a fine despite their admission of criminal activity. The defendants agreed to reimburse the full amount of over €5 million and were released from prison. ■

Scam call centres in Georgia have been known for lavish corporate-style parties. *Photo: Social media (account since deleted)*

Envirotech advertises a German-speaking sales specialist position. Responsibilities: Telephone communication with customers in our database. Salary: GEL1 500 plus bonuses (on average GEL3 000–GEL5 000). *Photo: Telegram*

Georgia also appears to be a better place for scammers to work. Recruitment has become more discreet in recent years, after a string of sting operations by journalists. Advertisements were previously posted extensively on social media and job websites,[134] but recruitment now happens in social circles, not social media. The employees are often students with language skills.[135] Unlike Ukraine, where staff turnover is high, Georgian call centres are keen to retain workers. One journalist said that 'those who overcome the morals stay a long time, as long as six years.'[136] Compared to Russia and Ukraine, employees are well rewarded, with an experienced team leader earning as much as US$30 000 a month.[137] High-performing scammers can earn up to US$20 000 a month, and call centre employees who extract the most money from victims are rewarded with various expensive gifts, including automobiles.[138]

Salaries at scam call centres in 2023 – when many of these call centres were operating – were generally higher than the 1 600 Georgian lari (GEL) (US$580) average salary in the formal employment market.[139] For example, employees of the conversion department at one scam call centre reported earning GEL4 000–GEL5 000 (US$1 400–US$1 800), and company managers received GEL10 000 (US$3 600). Retention department employees had exceptionally high compensation, with two surveyed members stating that their highest one-time payments were GEL80 000 (US$30 000) and GEL100 000 (US$37 000), respectively. Germany was reportedly their most lucrative target country, with victims regularly sending 'deposits' of 20 000–30 000 euros or dollars, although this may have changed recently.[140]

Georgian call centres also do not appear to have the climate of intimidation found in Ukraine, where successful scammers are prevented from quitting and it is impossible to work for a rival call centre network.[141] In Georgia, employees can, for the most part, leave freely and move between rival call centres with no consequences. [142] According to an investigative journalist, one employee set off a bidding war for her services, with two companies – her current and a rival – offering progressively higher salaries until she finally decided to move to the rival.[143] They also cited an audio recording of an employee who had moved to a rival with no consequences.[144] In the main, this speaks to an ecosystem that is competitive but also cooperative, with lessons and technology shared, resulting in a high degree of similarity in their operations. In the case of tech, for instance, both the AK and Milton groups used the Puma TS trading system, which was, according to charges filed by the Bavarian Cybercrime Unit, originally developed by the head of the Milton Group before being distributed to scam call centres worldwide.

Deepfakes: Projecting local credibility

AI is changing how scammers work. One of its most effective tools is the deepfake, the deployment of which often shows how sensitive scammers are to the social nuances of their targets, using images of prominent politicians, businesspeople, financial advisers, TV presenters and the like. Georgian scammers, for instance, have used deepfakes of a prominent financial adviser, a radio DJ and a broadcaster to scam money out of British clients.[146]

Armenia has also been the target of advertisements for investment schemes or fake gaming apps that feature deepfakes based on prominent public figures.[147] In 2025, Prime Minister Nikol Pashinyan was portrayed in at least two deepfakes connected to investment schemes.[148] Apparently, the first attempt was immediately exposed because the video deepfake spoke better Russian than Pashinyan did.[149] Scammers have even created deepfakes of the leadership of the Collective Security Treaty Organization, the regional body that, among other tasks, coordinates action against electronic fraud.[150]

In 2024, Meta developed an open-source tool for watermarking videos and is also testing a new automated review system to help combat the prevalence of celebrity-bait scams.[151] However, these efforts have come in for criticism for a lack of effectiveness and consistent implementation.[152]

Deepfake of Armenian Prime Minister Nikol Pashinyan, March 2025. *Photo: Screengrab from Aurora News, https://auroranews.am/news/2025-03-04-keghts-govazdayin-holovak-nikol-pashinyani-dimapatkerov*

One of the most alarming aspects in recent years has been the entrance of East Asian criminal actors who, according to the UN Office on Drugs and Crime, have established a fraud foothold in Batumi, Georgia.[145] Recruitment of Chinese nationals tricked into working in such centres – a key feature of scam call centres in South East Asia – points to a new paradigm, where Eurasian and East Asian ecosystems exist side by side and may begin to blur into one another.

Armenia: Rising from a low base

The call centre ecosystem in Armenia appears to be less developed than elsewhere in the region. In the first quarter of 2025, the central bank registered 408 cases of bank fraud.[153] Call centres are present, but not in significant numbers. Reports indicate that eight or nine operations were closed in the period from 2024 to mid-2025.[154] In other contexts, this low figure might signal that the industry is well protected, but interviewees in Armenia generally agreed that domestic operations were not on a serious scale and existed without political protection or connections to traditional organized crime.[155] Interestingly, one interviewee claimed that no significant local scamming economy had developed because people were able to put their skills into legal online gambling – echoing Israel's situation with binary options before 2017.

That said, Armenia has been experiencing greater scam activity for several years. The coronavirus pandemic pushed more people to e-commerce and opened the door for delivery-based scams, in which the victim is instructed to send money before an item can be delivered. These methods have grown more polished in recent years,[156] and were soon joined by others. In August 2024, the central bank issued a warning that socially engineered scams and phishing attempts were on the rise in Armenia.[157] That same month, the

media warned of a new type of scam: the fake emergency. Well-known in other parts of the region, this is when scammers ask for money to help the victim's relative, who they say is ill or has suffered an accident. Scammers had significant success with their new scheme, taking the equivalent of almost US$70 000 in just seven days[158] – a large haul in a country where the average annual income is approximately US$8 800.[159] In February 2025, two call centres, which had been scamming victims in Kazakhstan and European countries with an investment scheme, were shut down in Yerevan. Some 41 people were arrested, including citizens of Armenia, Georgia, Iran, Syria and Lebanon.[160] Such recent cases, while few in number, demonstrate the potential for sophisticated and networked operations.

In November 2025, Armenian law enforcement shut down a scam call centre that the ministry of internal affairs said was linked to other centres operating abroad.[161] According to a Georgian cybercrime expert interviewed in January 2026, Georgians were increasingly going to Armenia to set up scam operations, perhaps due to the cost of government 'overheads' in Georgia.[162]

Interviewees also pointed to an increase in scammers targeting Armenia from Ukraine and Russia after Russia's invasion of Ukraine.[163] Some have claimed that the exodus of Russians and Ukrainians from their home countries after February 2022 led to a 'new wave' in scamming,[164] but there is no credible evidence to establish whether this is a causal or coincidental connection. In an interesting twist, some scammers not only spoke Russian to their Armenian victims but also had insight into local features of Yerevan and its neighbourhoods to boost their credibility with the victims.[165] It is not clear whether they were calling from abroad or were locally based. It is also possible that the scammers were calling from other Russian-language speaking countries and had simply done their due diligence, such as by buying data on the dark web or scanning social media.

International employees

This report has considered scam call centres in the region in terms of individual countries, but it should be noted that they are often staffed by nationals of different countries. Like any company opening a new branch overseas, the directors of transnational scam networks can simply hire locals to do the scamming work while retaining overall control. To some degree, this explains the ability of call centres to transplant, as was the case with the Israeli operations moving into Georgia and elsewhere.

But it is also instructive that transnational call centres often hire far more widely than just locals, not least because of the language skills that international employees can bring. Many reports mention scammers and couriers who are citizens of countries within the region,[166] but some come from further afield, including Germany,[167] Turkey,[168] the Czech Republic[169] Latvia,[170] Iran, Syria and Lebanon.[171] The true reach of recruitment is unknown, as media reports often leave out such details for pretrial legal considerations,[172] but it is likely to be broad. The workers' conditions of employment in the region are not clear, nor whether there are signs of human trafficking, as has been seen with citizens of Russia, Uzbekistan, Kyrgyzstan and Kazakhstan in Myanmar.[173] ■

Country flags in a scam call centre raided by the Russian police in December 2024. *Photo: Screengrab from YouTube, https://www.youtube.com/shorts/R26_wc86AcQ*

THE BLACK BOX: WHERE CRIME AND POLITICS MEET

One of the most obscure aspects of the scam call centre economy in post-Soviet countries is the state provision of protection known as *krysha*, or 'roof'. The well attested involvement of officials in roofing various forms of organized crime is a legacy not only of the strong role of the state during Soviet times but also of the political trajectories of the former republics' transitions to independence after the collapse of the Soviet Union.[174] Criminal actors also provided such 'protection' during those turbulent times, imposing a modicum of order through extortion.

The evidence of this structural arrangement is, by nature, hard to determine: if the system is working well, then no evidence of wrongdoing is produced. Most assertions of state protection thus rely on inference. In some countries, ongoing crime is evidence of weak law enforcement. But where law enforcement agencies are strong and their influence pervasive, any flourishing of organized crime may be taken as indirect proof of official protection. Strong crime, in other words, relies on a strong state that is willing to look the other way, for a cut.

The level of this involvement is highly varied, from individual law enforcement and state officials to the heights of the state apparatus. This spectrum means that corruption can take many forms, from the simple acceptance of a bribe to the active direction of illicit activity in certain lucrative sectors or regions.

Allegations of corruption, however, must be parsed for political motivation, since claiming that a certain agency or ministry is involved in organized crime is a quick and headline-grabbing way to damage a political opponent. This is particularly the case in Georgia, where the government has been contending with claims of a rigged election in October 2024 and popular discontent with its pivot away from the path to European Union accession and towards a closer relationship with Russia.[175] All these caveats must be borne in mind when discussing state–criminal complicity.

The first observation to make is that the relationship between state and criminal actors varies across the region. In Armenia, for instance, where the scam call centre economy seems relatively nascent, there were no reports of state or law enforcement protection.[176] In Russia, the practice of *krysha* is widespread, with multiple cases of police officers convicted for facilitating or benefiting from various types of organized crime. [177] However, the GI-TOC was unable to find any open-source evidence of

scam call centres being protected by corrupt elements of the state, and other research paths are limited. There was also little evidence found in Central Asia.

There is stronger evidence in Ukraine and Georgia, albeit with the caveats mentioned above. In Ukraine, protection of scam call centres by corrupt law enforcement officials has been widely alleged in the media, by former employees and also by government officials.[178] The arrangement between corrupt law enforcement personnel and those running the call centres there was mostly described as transactional, with regular bribes being paid for non-interference. The call centres themselves were run by organized crime networks, including Khimprom.

The scheme in Georgia seems to be different, although it is harder to parse due to the political context. Interviewees broadly agreed that the link between the state and scammers existed – 'every call centre that operates in Georgia has a roof'[179] – but that the workings of that roof are murky. According to a Western diplomat, 'the state–crime nexus is there, but it's a black box for us.'[180]

Yet there was consensus among several interviewees that the involvement of the state was more direct than in the case of Ukraine, with government actors playing a leading role in the establishment and functioning of call centres (Figure 5). A Georgian cyber expert said that call centres that do not have this connection with the state are far more vulnerable to being shut down.[181] The most outspoken described scam call centres as a 'government operation'. In this analysis, criminals did not manage the call centre networks but provided informal security, essentially as intermediaries between the state and the call centre.[182] The multifaceted role of criminals – including one reportedly involved in the call centre world – as *titushki* (thugs hired to fight anti-government protesters) also highlights the strong connection between the state and crime.[183]

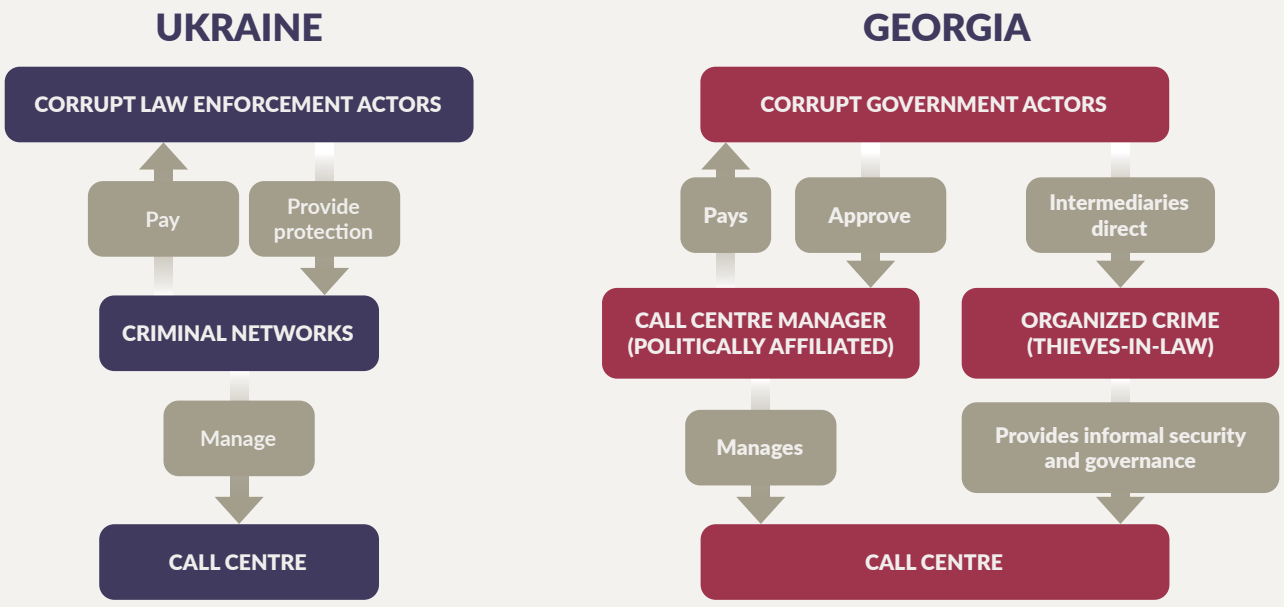


FIGURE 5 The various intersections between corrupt state actors and the scam call centre economy in Ukraine and Georgia.

The profits from call centres were described as black money for the ruling party, although it was acknowledged that there was no firm proof for this.[184] However, one interviewee said that the crackdown in October 2025 against businessman and former prime minister of Georgia Bidzina Ivanishvili's former inner circle was enabled by the fact that the officials under investigation were compromised by their involvement with scam call centres – an allegation supported by prosecutors in Georgia, who alleged that the former head of the State Security Service had received bribes from scam call centres in exchange for protection.[185] Georgia's former prime minister was also arrested for having 'secretly and covertly engaged in various types of business activities and received a particularly large amount of income of illegal origin' and sentenced to five years in prison as part of a plea deal.[186] Criminal cases have also been launched against the thieves-in-law and a former official allegedly directly involved in running the call centres, indicating that a changing of the guard may be underway.[187]

The state's close involvement makes investigation and discussion of scam centres extremely difficult: 'You can discuss any crime except call centres and "manifestations" [anti-government protests].'[188] This aspect was conspicuous during fieldwork in Tbilisi, where assurances of anonymity had to be given and interviews conducted in public places with background noise. There may not be court-ready evidence for state involvement in call centres, but this climate of anxiety is nevertheless suggestive.

Another indication of the state-crime nexus in Georgia is the track record of investigating and prosecuting call centres. According to one Georgian cyber security expert, no investigation is possible without an investigator checking up the chain of command first, to deputy minister or even ministerial level.[189] Many of the investigations into the major scam call centres in Georgia over the years are reactive, beginning after intensive journalistic investigations, and sometimes used for political purposes. Typically, prosecutions result in only minimal fines for the perpetrators – amounts that are significantly lower than the sums they have extorted. Speaking of international cooperation, one lawyer in Georgia said that local law enforcement 'don't resist [such efforts], but they do not take strict measures towards people [accused of the crime]'.[190]

In the case of Morgan Group, for example, the international investigation by a consortium of investigative journalists led to an official investigation. Information related to the case was often used for political purposes – in September 2024, for instance, a month before the parliamentary elections, authorities announced that the perpetrators had been arrested.[191] However, on 27 June 2025, the prosecutor's office reached a plea agreement with the defendants, imposing only a fine despite their admission of criminal activity, and all arrested individuals were released from prison.[192] The fines totalled approximately €5 million – a fraction of the scam's estimated true takings.[193] Interviews with lawyers revealed that these funds have not yet been paid to the victims. However, the prosecutor's office stated that once a request for the return of the funds is received from the relevant country's investigation, the money will be returned to the identified victims.

Notably, state agencies evidently knew about the scam centre as far back as 12 December 2019, when the financial police conducted a search at the Morgan Limited LLC offices at 10 Otar Chkheidze Street. The scam centre resumed operations at the same address within days,[194] and continued to operate for several years without significant intervention from law enforcement authorities.

Black Rock LLC and the AK Group, mentioned in the introduction above, offer more examples of failed investigations. On 9 April 2022, Mtavari Arkhi TV aired an interview with an individual who claimed to have worked at a Black Rock call centre.[195] The information provided was highly detailed and accurately described scam centre operations in Georgia.[196] After the interview, the prosecutor's

office initiated investigations against several individuals named by the anonymous source as operating and managing a fraudulent call centre, as well as engaging in money laundering.[197] These individuals were arrested and their assets frozen three consecutive times at the prosecutor's request, but they were then released. Tellingly, the shares of the Black Rock company were not frozen, indicating that it had not been investigated at all. As for the AK Group, the prosecutor's office has not issued any public statement regarding this high-profile case at the time of writing.

Ultimately, the strong level of political protection provides the scamming industry in Georgia with high levels of immunity. 'It's like a legitimate business here,' said one source with a shrug.[198]

GEOPOLITICS: A SCAMMER'S BEST FRIEND

Scam call centres also exploit international geopolitics. In Eurasia, the most dramatic development in recent years has been Russia's invasion of Ukraine, an event that has fundamentally reshaped many aspects of the region.

At the tactical level, the war presented scammers with new schemes that could be devised from emerging narratives, such as scams related to the Ukrainian and Russian military.[199] Ukrainian scammers, impersonating Russian officials, also accused Russian civilians of collaborating with or supporting the Ukrainian Armed Forces as a way to extort funds.[200]

On the macro scale, the Russo-Ukrainian war dealt a severe blow to international law enforcement cooperation. The transnational nature of scamming makes international cooperation essential to allow victim complaints to be used as evidence against criminals based abroad. As mentioned above, international cooperation in the sphere of call centres had already faced hurdles in Ukraine, Georgia and Russia, but the war raised them higher, playing into the hands of criminals. 'Criminals take advantage of lack of international cooperation,' commented one law enforcement liaison officer working in the region.[201]

In Ukraine, scammers began to target Russians much more heavily, safe in the knowledge that the complete lack of cooperation between Russia and Ukraine meant they would never be charged for their crimes. When asked about the legality of their activity, one Ukrainian scammer reflected, 'I wouldn't say it is legal, but it is not against the law.'[202] But the situation was very different when it came to Ukrainian scammers targeting Western countries, where law enforcement cooperation with Ukraine is strong. As the scale of the call centre phenomenon became more evident, Ukraine led a crackdown against scam call centres in mid-2023.[203] There are also signs of more stringent enforcement under Ukraine's new prosecutor general, Ruslan Kravchenko, who has been keen to put the issue of scams centre stage alongside Ukraine's willingness to work with international partners. Announcing the results of a crackdown on call centres in late 2025, he declared that 'international cooperation works, and the border is no longer a tool to hide from justice. Whoever deceives people in Ukraine or abroad will answer both in Ukraine and in Europe.'[204]

In Russia, international cooperation with the West had been very limited since the 2014 Russian annexation of Crimea and the Russian-backed insurgency in the Donbas. Since then, Russia has

The Russo-Ukrainian war has presented scammers with new opportunities, such as fake websites and appeals that falsely claim to be raising money for the armed forces or war efforts. *© Yasuyoshi Chiba/ AFP via Getty Images*

lamented that the 'refusal of Europeans' to cooperate is hindering its efforts to investigate scam call centres in Europe that have targeted both Russians and Europeans.[205] It also appears to be making efforts to build its own international cases, even without international cooperation. A December 2024 Russian media report interviewed several foreign victims of a Russia-based scam centre who had been flown in to Moscow, all expenses paid, to give their witness statements.[206] Given the timing – the half-hour news video was published only six days after the call-centre bust – it appears likely that the law enforcement and PR operations were closely coordinated. It is essential to bear in mind the political narrative that such efforts serve, painting Russia as the stalwart fighter of crime despite the lack of any Western assistance, including in cases where the victims are European.

The drift towards more authoritarian practices in some countries, including restrictions on the media in the shape of 'foreign agents' laws, also created a more amenable operating climate for scammers by protecting their activities from investigative journalists. In Georgia, Russia's invasion of Ukraine helped to catalyze a more authoritarian stance and closer ties to Russia.[207] Once on the path to EU accession, Georgia is now described as a candidate 'in name only'.[208] Domestically, the space for opposition and accountability has drastically shrunk, with most opposition figures either imprisoned, in exile or charged with criminal activity.[209] The Foreign Agents Registration Act passed in May 2024 – known locally as the 'Russia Law' – requires all NGOs that receive more than 20% of their funding from foreign donors to register as 'bearing the interests of a foreign power'.[210] It has had a similarly chilling effect on civil society and especially investigative journalism.

As the political climate changes, Western partners have found opportunities for engagement more limited, especially in terms of law enforcement.[211] Investigative journalism, which has done so much to shed light on the scam ecosystem in Georgia, will probably struggle to function unless based abroad, in turn removing the media 'push' factor that has often moved the state to launch official investigations, however lacklustre their results. This has created the perfect set of conditions for scammers, who are now insulated from international investigation and domestic scrutiny.

Asked what was needed to change to break this cycle, sources said the problem was not law enforcement, which seems to have the necessary capacity – 'If they want to solve something, they can'[212] – but the political environment. 'We cannot change anything until there is a political change,' said one journalist – a prospect that appears increasingly distant.[213]

CONCLUSION AND RECOMMENDATIONS

The combination of factors outlined above makes the scam call centre ecosystem in Eurasia a particularly hard challenge. Compounding the difficulty of tackling a highly sophisticated transnational criminal activity is a plethora of geopolitical factors that serve to protect the criminals from outsider interference. In this regard, scammers in Eurasia frequently have the best of both worlds: able to transcend borders to reach victims around the globe and to use those same borders as protection.

There are no easy fixes. For Western governments, international reach into Eurasia is limited or qualified, even in countries like Ukraine that have shown a willingness to partner on law enforcement issues. The state of play is also rapidly transforming. The telephone – or its VoIP equivalent – may still play a significant role, but is now just one weapon among many as scammers adopt AI and blend conventional cybercrime tools with social engineering. Scam call centres may look very different in a year or two. It could turn out that behemoths like the Milton Group and AK Group represent the peak of large-scale, people-led scamming; the future may belong to more lightweight tech-enabled operations in which the human scammer creates prompts, trains large language models and intervenes personally only to secure the transaction.

As such, the recommendations below are aimed at efforts that can clarify the nature of the problem, leverage what cooperation exists and point up the risks of some current responses.

International cooperation – rethinking the taboo?

One of the major impediments to tackling scam call centres operating out of Eurasia is the 'non-cooperation' wall between certain states in Eurasia and external governments, especially those from the West. The most prominent example of this is Russia, where international cooperation in the sphere of law enforcement is extremely challenging in the current political climate.

At present, reviving any form of cooperation with Russia is seen in many Western and like-minded circles as anathema, not only due to the full-scale invasion of Ukraine in 2022[214] but also the legacy of incidents such as the downing of Malaysia Airlines Flight 17, the poisoning of a former Russian spy and his daughter in the UK in 2018 (which also led to the death of a British citizen) and, more recently, concerns that Russia is misusing the INTERPOL Red Notice system to go after political opponents

abroad, and banning INTERPOL investigations in Russia.[215] Trust is in short supply, as highlighted by the terrorist attack on Crocus Hall in Moscow in March 2024. Despite the US warning its Russian counterparts of the attack a day before it happened, the advice was not heeded, and in the aftermath Russian officials publicly accused the West and Ukraine of involvement.[216]

Scam call centres are benefiting from this situation, able to effectively hide behind borders where law enforcement cannot reach them. Transnational cooperation is vital to changing this situation: as the Western law enforcement liaison officer said, 'Alone, we can't do anything.' [217]

Although not an easy sell to policymakers, there is an argument that there should be some form of negotiation at the operational level between law enforcement authorities in the region and outside it. Of course, this will not be a politics-free zone – Russia will, for example, have a clear interest in trying to target Ukraine-based scam call centres – but a limited, case-by-case engagement would arguably be preferable to none. This is not to undersell the very real concerns that exist among Western circles about engaging in the region, especially in terms of the necessity to present a unified front against Russian aggression, but at the same time there may be space to work, if the focus is clearly defined and expectations are managed. Above all, even if meaningful cooperation cannot be realized in the short term, it is vital to keep open what channels still remain to ensure the mechanism remains viable. 'Once you shut down the channels,' the liaison officer warned, 'it takes years to rebuild them.'[218]

It is also instructive that within the region, international cooperation to take down call centres is increasing and seemingly showing results. Russia, Kazakhstan, Belarus, Kyrgyzstan and Uzbekistan have expanded their mutual cooperation in recent years, which led to the dismantling of at least one transnational network in the region in 2024–2025.[219] It may be that a wider initiative involving regional states and Western partners may be a more palatable vehicle for cooperation in political terms, rather than bilateral partnerships.

Coordinate leverage and change scammer's risk calculus

Building cases against scam call centres is difficult. Victim testimony is required, which may not be forthcoming due to accessibility issues or a sense of shame. International investigations require cooperation between partner states, which as this report has illustrated, can also prove problematic. The use of tech and sophisticated money laundering techniques also greatly complicates the work of investigators. According to one cybercrime expert who formerly worked in criminal justice, investigators are reluctant to investigate a case for longer than a month, and the maximum term permitted to bring a case to trial before a suspect is released – nine months – is no time at all, given the complexity of such cases.[220]

With so many factors weighing against a prosecution, it is clear that states need to coordinate across different points to bring sufficient pressure, particularly when dealing with states where scam call centres benefit from protection. These points may entail partnering with other target countries to collect international victim testimony, exerting pressure through diplomatic channels, and taking to task websites that are used by scammers as interfaces, including by sanctioning them. Flagship law enforcement operations that seek to put boots on the ground can also help change the risk assessment of scammers, as has been seen in Georgia, where scammers are now wary of targeting Germans after the German law enforcement operation there.[221]

As such, a coordinated strategy across government and between governments into flagship cases may meaningfully change a scammer's calculation of risk. That said, it must be acknowledged that

such an approach does simply displace the scamming elsewhere, and cannot work where countries do not have a point of entry with the country of origin (such as Western governments with Russia).

Tackle upstream fraud architecture

As this report has illustrated, Western states – frequently the victims of scam call centres in Eurasia – often have limited agency when it comes to pursuing such cases. The one exception to this, however, is the realm where victims first interact with scammers – often social media sites such as Facebook or Instagram, which generally are headquartered in the West (Russia's Max and Telegram being notable exceptions).

Cracking down on scam adverts on social media sites is critical to avoid victims connecting with scammers, but the scale of this challenge is vast, for two reasons. The first is scale. AI allows for the instant generation of countless adverts, both still images and videos, all tailored for a target audience. Some may only stay live for a few hours before being replaced by another version, subtly tweaked.[222]

The response of tech giants to the issue is also suboptimal. While social media giants like Meta claim they are making every effort to tackle the problem, investigators and watchdogs often point to lengthy lags before action is taken against scam advertisements, if at all.[223] In a widely discussed report, internal Meta documents seen by Reuters estimated that the tech company would earn approximately 10% of its overall annual revenue, or US$16 billion, from advertising for scams and banned goods – with users exposed to 15 billion scam ads a day – although these figures were disputed by a Meta spokesperson as 'rough and overly-inclusive', and that the actual number was lower.[224]

The discussion over tech companies' responsibilities for the content they host is as old as the companies themselves, but the scale and lucrative nature of the issue should surely push this up the policy agenda. At present, there exists a strange disjunct whereby a dropper whose account is used faces more criminal risk – and indeed, in some countries is liable for the amount scammed – than a tech company that acts as a vital shop window for scammers.

New legislation required, but beware infringing civil rights

Given the difficulty of bringing scammers to book, it may be that new legislation is required. Simplifying the evidential burden, streamlining investigations and enabling law enforcement to act in a proactive manner to scams would increase citizen security. But as trends in Eurasia show, legislation can be a double-edged sword, with many of the same tools that can combat communication-facilitated scams having the potential to enhance state surveillance and control of society.

Of all the countries in the region, Russia has made arguably the greatest moves to tackle scam call centres, although others have also stepped up their response.[225] Since 2021, Russia has introduced a range of measures, from greater bank responsibility in detecting suspicious transaction patterns and the ability to freeze payments to a ban on sending an SMS message while a call is in progress.[226] Sberbank is also calling for harsher penalties against scammers who use deepfakes.[227]

The response with the most significant political implications is the targeting of 'spoofing', or scammers manipulating their numbers to make it appear that they are calling locally. In December 2022, Roskomnadzor launched the Antifraud system to block calls on the traditional phone network that showed signs of spoofing. Russia's success at blocking spoofing practices has been mixed – while the state declared that the system blocks hundreds of millions of spoofed call a year,[228] it is clear that

workarounds (such as SIM boxes) have already developed, allowing scammers (with the help of local facilitators) to bypass call authentication frameworks and use local Russian numbers.[229] Similar cases have also been reported in Belarus.[230]

This in turn had led the state to start imposing limits on the purchase of SIM cards and initiate verification procedures (as scammers use duplicate SIM cards to get authentication codes).[231] But Russia has also gone much further, using the spectre of spoofing to block calls on WhatsApp and Telegram in August 2025.[232] It also launched a new national messenger called Max, which comes pre-installed on any new smartphone (ironically, it has already been the target of scammers).[233] This has caused consternation among many, who read Russia's anti-scam measures as a stalking horse for greater government oversight and information control, especially in the occupied territories of Ukraine and among foreign citizens in Russia, who now have to provide biometric information to buy a SIM card.[234] Max – sometimes referred to in the media as 'Russia's WeChat' (the Chinese state-developed application) – collects certain kinds of user data and reserves the right to share it with third parties and government agencies.[235] There has been strong pushback against claims about Max's potentially nefarious uses in the Russian media, although this in turn may be part of a public messaging drive.[236]

Similar risks apply in Georgia, where one Western diplomat said that collaboration on cyber-solutions to tackle fraud was a non-starter, given the risks that such tools could be repurposed for political ends.[237]

Notably, Russia's efforts have not turned the tide, with the deputy chair of Sberbank predicting that fraud would rise by 15%–20% in 2025.[238] This may provide further justification for more sweeping legislation, with additional consequences for civil rights. Of course, this risk is not limited to Russia: in any state, Eurasia or elsewhere, scams may serve as a useful justification for restrictive practices. Balancing such risks must be a key part of the conversation in any response formulation.

NOTES

1 James Dowsett, Exposed Tbilisi call center scammers delete social media accounts, Organized Crime and Corruption Reporting Project (OCCRP), 5 March 2025, https://www.occrp.org/en/news/exposed-tbilisi-call-center-scammers-delete-social-media-accounts.

2 Alexander Kupatadze, Den of thieves: Mapping organized crime in the South Caucasus, GI-TOC, August 2025, p 14, https://globalinitiative.net/analysis/den-of-thieves-mapping-organized-crime-in-the-south-caucasus.

3 Kristina Amerhauser and Audrey Thill, The business of exploitation: The economics of cyber scam operations in Southeast Asia, GI-TOC, August 2025, https://globalinitiative.net/analysis/cyber-scam-operations-southeast-asia; Sasha Jesperson, Trafficking into forced criminality: The rise of scam centres in Southeast Asia, RUSI, 18 January 2024, https://www.rusi.org/networks/shoc/informer/trafficking-forced-criminality-rise-scam-centres-southeast-asia.

4 For example, OCCRP, Trail of broken lives leads to Kyiv call center, 2 March 2020, https://www.occrp.org/en/project/fraud-factory/trail-of-broken-lives-leads-to-kyiv-call-center; OCCRP, Web of call-center 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, Behind the scam: How fraudsters use social media, software, and shell companies to steal millions, 25 July 2025, https://www.occrp.org/en/investigation/behind-the-scam-how-fraudsters-use-social-media-software-and-shell-companies-to-steal-millions; OCCRP, Diamonds, Dior and Dubai vacations: The luxurious lives of Georgia's call-center scammers, 5 March 2025, https://www.occrp.org/en/project/scam-empire/diamonds-dior-and-dubai-vacations-the-luxurious-lives-of-georgias-call-center-scammers.

5 A brief survey of recent trends is provided in Luke Rodeheffer, Call center scams spread across Eurasia, Eurasia Daily Monitor, Jamestown Foundation, 24 July 2025, https://jamestown.org/program/call-center-scams-spread-across-eurasia.

6 For instance, INTERPOL posits South East Asia as 'the original "hub" region' for scam call centres enabled by human trafficking before the model spread globally. INTERPOL, INTERPOL releases new information on globalization of scam centres, 30 June 2025, https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres. A 2025 report by the UN Office on Drugs and Crime (UNODC) also explores the spread of 'illicit activity involving Asian crime syndicates' related to fraud in the Pacific, Africa, South America and South Asia. UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, pp 8–11, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

7 According to the UNODC, East Asian criminal actors have sought to establish a fraud foothold in Batumi, Georgia. UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, p 61, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf. See also: OCCRP, The phantom investor: How a wanted meth kingpin posed as a tycoon in Georgia, 21 January 2026, https://www.occrp.org/en/investigation/the-phantom-investor-how-a-wanted-meth-kingpin-posed-as-a-tycoon-in-georgia. On Eurasian transnational organized crime groups with interests in Myanmar: Interview with an MP, Kyiv, Ukraine, February 2025.

8 Reuters, Israel ban on binary options gets final parliamentary approval, 23 October 2017, https://www.reuters.com/article/business/israel-ban-on-binary-options-gets-final-parliamentary-approval-idUSKBN1CS2L0; Simona Weinglass, Israeli ministers approve bill to outlaw entire binary options industry, *Times of Israel*, 18 June 2017, https://www.timesofisrael.com/israeli-ministers-approve-bill-to-outlaw-entire-binary-options-industry.

9 The size of the market share is supported by estimates from SpotOption and TechFinancials, two Israeli brokerage firms that handled the majority of trades for binary options, together handling US$8 billion per year. SpotOption was later charged with fraud by the US Securities and Exchange Commission. Simona Weinglass and David Horovitz, Don't

let Israel become a promised land of impunity for crooks and fraudsters, *Times of Israel*, 1 July 2018, https://www.timesofisrael.com/dont-let-israel-become-the-promised-land-of-impunity-for-crooks-and-fraudsters; Tova Cohen and Luke Baker, Special report: From Israel via London, an online gambling scam traps thousands, Reuters, 27 September 2016, https://www.reuters.com/investigates/special-report/israel-investing-binary; US Securities and Exchange Commission, SEC charges binary options trading platform and two top executives with fraud, 19 April 2021, https://www.sec.gov/newsroom/press-releases/2021-66.

10 Tova Cohen and Luke Baker, Special report: From Israel via London, an online gambling scam traps thousands, Reuters, 27 September 2016, https://www.reuters.com/investigates/special-report/israel-investing-binary.

11 Marcos García Rey, *De Kiev a España: 'calls centers' del Este, investigados por vaciar miles de cuentas*, *El Confidencial*, 1 March 2020, https://www.elconfidencial.com/espana/2020-03-01/chiringuitos-financieros-fraude-inversion-criptomonedas_2475391.

12 Ibid

13 Simona Weinglass, Israeli-run scam in Kyiv shows how binary options industry has mutated, *Times of Israel*, 18 March 2020, https://www.timesofisrael.com/israeli-run-scam-in-kyiv-shows-how-binary-options-industry-has-mutated/.

14 Interview with a journalist, June 2025, online.

15 Graham Stack and James Dowsett, German court sentences key figure in massive call center scam operation exposed by OCCRP, OCCRP, 27 February 2026, https://www.occrp.org/en/news/german-court-jails-key-figure-in-massive-call-center-scam-operation-exposed-by-occrp.

16 Simona Weinglass, German prosecutors take aim at Israelis behind 77 million euro fraud ring, *Times of Israel*, 3 July 2023, https://www.timesofisrael.com/german-prosecutors-take-aim-at-israelis-behind-77-million-euro-fraud-ring; Bavarian Attorney General's Office, Following extradition from France: further charges against the alleged person responsible for the fraudulent cyber trading platform GetFinancial have been filed with the Regensburg Regional Court, 26 June 2024, https://www.justiz.bayern.de/gerichte-und-behoerden/generalstaatsanwaltschaft/bamberg/presse/2024/9.php.

17 According to documents from the prosecutor's office seen by an investigative journalist in Georgia, legislative restrictions in Israel prompted Envirotech to move from Israel to Georgia.

18 Documents from the Georgian prosecutor's office, seen by an investigative journalist in Georgia.

19 OCCRP, Everything you needed 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. For Serbia, see: Sasa Dragojlo and Maxence Peigne, Boiler room: Belgrade call centres at heart of Israeli-linked investment scam, Balkan Insight, 30 September 2025, https://balkaninsight.com/2025/09/30/boiler-room-belgrade-call-centres-at-heart-of-israeli-linked-investment-scam. For Bulgaria, see: Simona Weinglass, Alleged Israeli financial scammer arrested in Bulgaria, *Times of Israel*, 7 March 2019, https://www.timesofisrael.com/alleged-israeli-financial-scammer-arrested-in-bulgaria. For Cyprus, see: *Financial Mirror*, Cyprus call centre served as hub in fraud ring, 6 March 2025, https://www.financialmirror.com/2025/03/06/cyprus-call-centre-served-as-hub-in-fraud-ring.

20 See, for instance, Federico Varese, *Mafias on the Move: How Organized Crime Conquers New Territories*. Princeton: Princeton University Press, 2011.

21 Interview with an NGO, Tbilisi, Georgia, October 2025; Kreston Global, Doing business in Georgia, https://www.kreston.com/doing-business-in/georgia.

22 Brand Ukraine, Doing business in Ukraine, https://ukraine.ua/invest-trade/doing-business-in-ukraine.

23 Mtavari Arkhi, **ნიკა გვარამიას ექსკლუზიური ინტერვიუ | ე.წ. ქოლცენტრების სქემის სრული ანატომია,** YouTube, 9 April 2022, https://www.youtube.com/watch?v=mmXTggq1Mbw.

24 Tbilisi City Court, Decision on freezing assets, 23 January 2023; Tbilisi City Court, Decision on freezing assets, 18 January 2024; Tbilisi City Court, Decision on freezing assets, 16 January 2025.

25 Black Rock LLC, Business documents [Official corporate record], 11 June 2020.

26 This figure was cited by OCCRP according to the 'financial records of managers of the Georgian operation'. Civil.ge, Journalists expose global scam operating out of Tbilisi, 6 March 2025, https://civil.ge/archives/667514.

27 OCCRP et al, **ქოლ-ცენტრის ქართული "იმპერია**", iFact, 5 March 2025, https://ifact.ge/gaitsanit-skameri.

28 Tamta Kakhaberidze, **თაღლითობა და ფულის გათეთრება – A.K. Group-ის ქოლ-ცენტრ საქმეზე პროკურატურამ გამოძიება დაიწყო**, NetGazeti, 7 March 2025, https://netgazeti.ge/news/766761.

29 GI-TOC, Kyiv calling: The scam call centre phenomenon in Ukraine, forthcoming.

30 In Russia, for instance, independent researchers claim almost 90% of all Russians have experienced telephone fraud. 1Prime, The causes of most financial fraud attempts have been revealed, 22 September 2024, https://1prime.ru/20240922/moshennichestva-851704430.html.

31 Riza Turdakynyzy, Шетелдік интернет алаяқтардың алдауына түскен қазақстандықтар 5,8 млрд теңгеге кредит рәсімдеп, 7 млрд теңге шығынға батқан, Kursiv, 20 October 2023, https://kz.kursiv.media/kk/2023-10-20/rztq-internetalayaq; Abror Tovmurodov, *Ichki ishlar vazirligi telefon firibgarligi haqida ogohlantirdi*, Zamín, 6 November 2025, https://zamin.uz/uz/jamiyat/167527-ichki-ishlar-vazirligi-telefon-firibgarligi-haqida-ogohlantirdi.html;

Interview with a former World Bank official and an organized crime expert, Yerevan, Armenia, October 2025.

32 Ilya Varmalov, Мошенники: как россиян лишают миллиардов | Тюремные колл-центры, офисы в Украине, нейросети, даркнет, YouTube, 1 April 2025, https://www.youtube.com/watch?v=6dRA71QdSCY&t=2506s. Journalists who had investigated the Milton Group said that they only came across two Georgians who had been scammed, and both were scammed by the branch in Kyiv. Interview with investigative journalists, Tbilisi, Georgia, October 2025.

33 See, for example, Sanket Badhe, Scam agents: How AI agents can simulate human-level scam calls, arXiv, 8 August 2025, https://arxiv.org/pdf/2508.06457; Thomas Claburn, Voice-enabled AI agents can automate everything, even your phone scams, The Register, 24 October 2024, https://www.theregister.com/2024/10/24/openai_realtime_api_phone_scam.

34 Interview with an MP, Kyiv, Ukraine, February 2025.

35 Interview with L, a former employee of a scam call centre, February 2025; interview with the Ukrainian Interbank Payment Systems Member Association (EMA), Kyiv, Ukraine, July 2025; 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.' For an example of one such network, see: 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.

36 Ukrainian National News, "Від слів до справ": Кравченко повідомив про викриття у межах міжнародної співпраці схеми наживи шахраїв на громадянах ЄС на близько $250 тисяч, 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.

37 TASS, IT executive says 80% of phone fraud in Russia originates from Ukraine, 3 December 2024, https://tass.com/economy/1881075.

38 For other instances of Russian call centres linked to Ukraine, see Federal Security Service of the Russian Federation, ФСБ России совместно с МВД России пресечена противоправная деятельность действовавшей в Московской, Новосибирской, Томской областях и Алтайском крае организованной группы лиц, причастной к дистанционному мошенничеству в отношении граждан РФ, 25 July 2025, http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10440347%40fsbMessage.html; Interfax, FSB reports detaining 5 people in Russia in connection with fraudulent Ukrainian call center, 8 April 2024, https://www.interfax-russia.ru/military/news_eng/406486.

39 1TV, В Москве раскрыта масштабная сеть мошеннических колл-центров, 11 December 2024, https://www.1tv.ru/news/2024-12-11/495168-v_moskve_raskryta_masshtabnaya_set_moshennicheskih_koll_tsentrov.

40 TVP World, Russia's 'Bitmama' jailed in penal colony for €20 mln cryptocurrency scam, 27 June 2025, https://tvpworld.com/87506467/russias-bitmama-jailed-for-20m-cryptocurrency-scam.

41 Interfax, Начальник УБК Москвы: ущерб от киберпреступлений исчисляется десятками миллиардов рублей, 19 October 2025, https://www.interfax.ru/interview/1053401.

42 For an example of Ukrainian claims that Khimprom is a Russian organization directed by the Russian security services, see Security Service of Ukraine, З початку повномасштабної війни СБУ знешкодила понад 60 злочинних угруповань, які планували перетворити Україну на транзитера наркотиків до ЄС, 28 December 2023, https://ssu.gov.ua/novyny/z-pochatku-povnomasshtabnoi-viiny-sbu-zneshkodyla-ponad-60-zlochynnykh-uhrupovan-yaki-planuvaly-peretvoryty-ukrainu-na-tranzytera-narkotykiv-do-yes-video. For Russian claims that it started in Ukraine and is directed by the Ukrainian security services, see URA.ru, RAN: РИАН: Верховная рада прикрывала крупную ОПГ, торгующую наркотиками в РФ, 31 October 2023, https://ura.news/news/1052699417. On drugs as a 'tool of war' in Ukraine, see Ruggero Scatturo, The devil's not-so-new psychoactive substance, GI-TOC, 23 May 2023, https://globalinitiative.net/analysis/alfa-pvp-drug-trafficking-ukraine-russia-conflict.

43 In 2017, a Russian court convicted Khimprom members for synthetic drug trafficking, with a production capacity estimated at 150–500 kilograms per week. Marina Sovina, Суд в России вынес приговор членам международного наркосиндиката, Lenta, 8 October 2022, https://lenta.ru/news/2022/10/08/himprom. On Khimprom activity in Ukraine since 2014, see Security Service of Ukraine, З початку повномасштабної війни СБУ знешкодила понад 60 злочинних угруповань, які планували перетворити Україну на транзитера наркотиків до ЄС, 28 December 2023, https://ssu.gov.ua/novyny/z-pochatku-povnomasshtabnoi-viiny-sbu-zneshkodyla-ponad-60-zlochynnykh-uhrupovan-yaki-planuvaly-peretvoryty-ukrainu-na-tranzytera-narkotykiv-do-yes-video.

44 UNODC, Ukraine: Organized crime dynamics in the context of war, July 2025, https://www.unodc.org/documents/dataand-analysis/Ukraine/Ukraine_OC_Study.pdf; on presence in Myanmar: Interview with an MP who served on a commission investing scam call centres, Kyiv, Ukraine, 2025.

45 Yulia Vorobyeva, Crossroads: Kazakhstan's changing illicit drug economy, GI-TOC, October 2023, https://globalinitiative.net/analysis/kazakhstans-illicit-drug-economy.

46 On the 280 'black' call centres in the prison system, see: Alena Sukharevskaya, Alexey Nikolsky and Pavel Kantyshev, Как заключенные охотятся за деньгами клиентов российских банков, Vedomosti, 13 November 2018, https://www.vedomosti.ru/finance/articles/2018/11/13/786367-kak. On Ukraine, see for example: EurAsia Daily, Дело о кредитном мошенничестве: задержаны 16 подозреваемых Подробнее, 7 November 2019, https://eadaily.com/ru/news/2019/11/07/delo-o-kreditnom-moshennichestve-zaderzhany-16-podozrevaemyh; Interfax, В Московском регионе задержали организаторов мошеннического "колл-центра", 29 October 2020, https://www.interfax.ru/moscow/734744. For more on prison call centres, see: VGTRK journalist: The Federal Penitentiary Service has declared war on prison 'call centres', Vesti, 11 December 2020, https://www.vesti.ru/article/2497682.

47 Ilya Varlamov, Мошенники: как россиян лишают миллиардов | Тюремные колл-центры, офисы в Украине, нейросети, даркнет, YouTube, 1 April 2025, timestamp approx. 26:40, https://www.youtube.com/watch?v=6dRA71QdSCY&t=2506s.

48 Sberbank, Телефонный развод. В борьбе с мошенниками-«звонарями» необходим комплексный подход, n.d., https://www.sberbank.ru/ru/person/kibrary/experts/borba_s_telefonnim_razvodom.

49 Pravo, Banks warn of new fraud schemes during COVID-19, 24 April 2020, https://pravo.ru/news/221027.

50 RBC, Вот сколько персональных данных россиян слили в Сеть с начала 2025 года, 23 September 2025, https://www.rbc.ru/life/news/68d26aaf9a794747a147fe5c.

51 *Izvestia*, Alarm bells: Putin declared unacceptable scale of fraud in the Russian Federation, 3 May 2025, https://iz.ru/en/node/1849375.

52 *Kommersant*, МВД перечислило самые распространенные у мошенников схемы обмана россиян, 22 November 2025, https://www.kommersant.ru/doc/8228192.

53 Ilya Varlamov, Мошенники: как россиян лишают миллиардов | Тюремные колл-центры, офисы в Украине, нейросети, даркнет, YouTube, 1 April 2025, timestamp approx. 26:40, https://www.youtube.com/watch?v=6dRA71QdSCY&t=2506s

54 Ibid, timestamp approx. 28:45.

55 Ilya Varlamov, Мошенники: как россиян лишают миллиардов | Тюремные колл-центры, офисы в Украине, нейросети, даркнет, YouTube, 1 April 2025, timestamp approx. 28:45; *Izvestia*, The average salary in Moscow increased by 13%, 29 May 2025, https://en.iz.ru/en/1894580/2025-05-29/average-salary-moscow-increased-13.

56 Conversation with investigative journalist, by Signal, December 2025.

57 Alexey Posttaruk, В МВД России назвали число людей, вовлеченных в мошеннические схемы, *Gazeta*, 11 February 2025, https://www.gazeta.ru/social/news/2025/02/11/25052750.shtml.

58 RBC, Подросткам запретили оформлять карты: меры борьбы с дропперами, 19 September 2025, https://www.rbc.ru/quote/news/article/67b4786b9a794706bc7706bd.

59 RBC, Подросткам запретили оформлять карты: меры борьбы с дропперами, 19 September 2025, https://www.rbc.ru/quote/news/article/67b4786b9a794706bc7706bd; Bulletin of the Russian Cyber Police, Если вашему ребенку ещё нет 14, а у него уже есть собственные деньги, пора, как минимум, насторожиться, Telegram, 27 May 2025, https://t.me/cyberpolice_rus/3672. See also Bank of Russia: Методические рекомендации Банка России о повышении внимания кредитных организаций к отдельным операциям клиентов – физических лиц, 17 September 2025, https://cbr.ru/Crosscut/LawActs/File/10091.

60 RBC, Подросткам запретили оформлять карты: меры борьбы с дропперами, 19 September 2025, https://www.rbc.ru/quote/news/article/67b4786b9a794706bc7706bd.

61 Sofia Tokareva, Уголовный перевод: какое наказание грозит дропперам по новому закону, *Izvestia*, 20 June 2025, https://iz.ru/1907429/sofiia-tokareva/ugolovnyi-perevod-kakoe-nakazanie-grozit-dropperam-po-novomu-zakonu; Ulpan Sabi, New criminal article on transferring bank cards comes into effect in Kazakhstan, Tengri News, 16 September 2025, https://en.tengrinews.kz/kazakhstan_news/new-criminal-article-on-transferring-bank-cards-comes-into-269435; Legal Information, Penalties for crimes in the field of information technology will be strengthened, Telegram, 6 May 2025, https://t.me/huquqiyaxborot/17926.

62 Tatyana Voronoa, Дропперы сократили средний размер транзакций в 10 раз, Frank Media, 26 September 2025, https://frankmedia.ru/220746.

63 Interfax, Начальник УБК Москвы: ущерб от киберпреступлений исчисляется десятками миллиардов рублей, 19 October 2025, https://www.interfax.ru/interview/1053401.

64 The official Telegram channel of the Criminal Investigation Department of Russia's Ministry of Internal Affairs.

65 Bulletin of the Russian Cyber Police, Золото вместо перевода, Telegram, 31 January 2025, https://t.me/cyberpolice_rus/3031.

66 See, for example, Onliner, Подробности дела пенсионерки, которая выбросила из окна 760 тысяч евро курьеру мошенников, 9 June 2024, https://money.onliner.by/2024/06/07/podrobnosti-dela-pensionerk.

67 Bulletin of the Russian Cyber Police, Чем заканчивается, когда колл-центр отправляет в “командировку”, Telegram, 5 June 2025, https://t.me/cyberpolice_rus/3708.

68 MK, В России увеличилось количество краж из-за прикладывания банковской карты к смартфону, 8 March 2025, https://kavkaz.mk.ru/social/2025/03/08/v-rossii-uvelichilos-kolichestvo-krazh-izza-prikladyvaniya-bankovskoy-karty-k-smartfonu.html.

69 ‘Pig butchering’, which alludes to pigs that are fattened up before slaughter, involves scammers establishing a relationship with a victim over days, weeks or even months, before persuading them to send large sums of money, whereupon the relationship is usually terminated.

70 *Gazeta*, Россиянам рассказали о необычной «романтической» схеме мошенничества на крипторынке, 10 June 2025, https://finance.mail.ru/article/rossiyanam-rasskazali-o-neobychnoy-romanticheskoy-sheme-moshennichestva-na-kriptorynke-66509564.

71 VK, Романтическое мошенничество: что это и почему ИИ выводит его на новый уровень, 18 November 2024, https://vk.com/@futurecrew-romanticheskoe-moshennichestvo-chto-eto-i-pochemu-ii-vyvodit; C-News, RED Security SOC: объем фишинга с использованием ИИ вырос на 53%, 19 September 2025, https://www.cnews.ru/news/line/2025-09-19_red_security_soc_obem_fishinga_s.

72 Yana Avezova, Roman Reznikov and Valery Besedin, Code Red 2026: Актуальные киберугрозы для российских организаций, 8 October 2025, https://ptsecurity.com/research/analytics/russia-cyberthreat-landscape-2026/#id2.

73 *Kommersant*, Детей втягивают в схемы, 25 August 2025, https://www.kommersant.ru/doc/7989337; Kaspersky Team, How scammers attack young gamers, Kaspersky Daily, 6 September 2024, https://www.kaspersky.co.uk/blog/how-scammers-attack-young-gamers-2024/28135.

74 Luke Rodeheffer, Call center scams spread across Eurasia, Eurasia Daily Monitor, 22, 109, 24 July 2025, https://jamestown.org/program/call-center-scams-spread-across-eurasia.

75 TASS, Damage from phone scammers in Russia exceeded $2.1 bln in 2024 – FSB, 7 May 2025, https://tass.com/society/1954527.

76 Smotrim, Сбербанк: по итогам 2024 года мошенники украли у россиян не менее 295 млрд руб, 6 June 2025, https://smotrim.ru/article/4537994.

77 PlusWorld, Fraudsters in Russia make 5-6 million calls on average per day in 2025, 9 June 2025, https://plusworld.org/daily/fraudsters-in-russia-make-5-6-million-calls-on-average-per-day-in-2025.

78 Interfax, Начальник УБК Москвы: ущерб от киберпреступлений исчисляется десятками миллиардов рублей, 19 October 2025, https://www.interfax.ru/interview/1053401.

79 EurAsia Daily, A group of fraudsters with a daily turnover of 10 million was neutralized in the Moscow region – Ministry of Internal Affairs, 19 September 2025, https://eadaily.com/en/news/2025/09/19/a-group-of-fraudsters-with-a-daily-turnover-of-10-million-was-neutralized-in-the-moscow-region-ministry-of-internal; RIA Novosti, Трех жителей Дагестана заподозрили в пособничестве кол-центрам мошенников, 2 September 2025, https://ria.ru/20250902/zaderzhanie-2039196491.html; 1Prime, https://1prime.ru/20250716/fsb-859540670.html, 16 July 2025, https://1prime.ru/20250716/fsb-859540670.html.

80 Ministry of Internal Affairs Media, Следователем СУ УМВД России по г.о. Коломна ..., Telegram, 18 September 2025, https://t.me/mediamvd/42060.

81 On rising fraud in Belarus: ‘Over the first nine months of 2024, fraud accounts for more than 55% [of all criminal offences], or more than half. There are two main forms of deception: under the pretext of selling a product or service (40%) and under various pretexts during calls or posing as bank or law enforcement employees (21%). Moreover, 35% of all cyber frauds were committed using Instagram under the pretext of selling goods. Viber accounted for more than 14%. Telegram was used in 26% of crimes committed, and WhatsApp – 7% .’ Investigative Committee of Belarus, Telegram, 27 November 2024, https://t.me/skgovby/12176; Ministry of Internal Affairs: 40% of cyber fraud occurs on social networks, Refrom News, 27 November 2024, https://reform.news/mvd-40-kibermoshennichestv-prihodjatsja-na-socialnye-seti.

82 Council of Europe, Belarus: Cybercrime, https://www.coe.int/en/web/cybercrime/institutions_by.

83 BelTA, Belarus’ cybercrime-fighting methods attract attention in non-CIS countries, 13 November 2025, https://eng.belta.by/society/view/belarus-cybercrime-fighting-methods-attract-attention-in-non-cis-countries-173511-2025.

84 BelTA, Ministry of Internal Affairs reports decrease in cybercrime in Belarus, 5 November 2025, https://eng.belta.by/society/view/ministry-of-internal-affairs-reports-decrease-in-cybercrime-in-belarus-173269-2025.

85 F6, AntiFraud Club: AntiFraud Club: за год в Беларуси предотвращено более 30 000 случаев мошенничества, 28 November 2025, https://www.f6.ru/media-center/press-releases/antifraudclub.

86 Daria Bernstein, Как власти Беларуси манипулируют цифрами о преступности, DW, 12 February 2025, https://www.dw.com/ru/kak-vlasti-belarusi-manipuliruut-ciframi-o-prestupnosti/a-71588183.

87 Losses due to fraudulent card activity, while not an exact measure of scam call centre activity (as it will include other kinds of fraud, and does not capture transactions the victim makes voluntarily), nevertheless does capture instances in which scammers gain access to the victim’s bank accounts, which is a key tactic of scam call centres.

88 How much money the fraudsters took from Belarusians, the National Bank said, Tochka, 28 October 2025, https://tochka.by/articles/economics/skolko_deneg_moshenniki_uveli_u_belorusov_rasskazali_v_natsbanke. Some 93% of these losses were due to social engineering frauds: Nina Atteza, You've probably often heard stories about scammers stealing money remotely. The National Bank has revealed the scale of the problem—the amount involved can be staggering, Zerkalo, 29 October 2025, https://news.zerkalo.io/economics/112126.html.

89 Olga Prokopyeva, A Minsk resident lost $900 thousand, other Belarusians - millions of rubles. Top 10 scams of recent years, Onliner, 22 October 2025, https://money.onliner.by/2025/10/22/top-10-afer.

90 It must be caveated that the data is not uniform. While data relating to fraudulent card transactions in 2024 was available for Russia and Ukraine, data had to be extrapolated for Belarus (data only available for Q3 2025 losses) and Kyrgyzstan (data only available for Q1 and Q2 2024). For Ukraine, see: Interfax, Loss from fraudulent card transactions in 2024 increases by 37% while their number decreases by 1% – NBU, 12 May 2025, https://en.interfax.com.ua/news/economic/1071180.html; for Russia, see: *Izvestia*, Fraudsters stole 27 billion rubles from Russians in 2024, 18 February 2025, https://en.iz.ru/en/1841157/2025-02-18/fraudsters-stole-27-billion-rubles-russians-2024; for Kyrgyzstan, see: Mariia Indina, Thefts from bank cards are on the rise: Kyrgyz citizens have lost more than 15 million KGS in six months, Akchabar, 30 September 2024, https://www.akchabar.kg/en/article/ekonomika-fmluaeuoncqnjkhr/rost-krazh-s-bankovskikh-kart-za-polgoda-kirgizstantsi-poteryali-bolee-15-mln-somov-cvkqbgtmsfbqaprm; for Belarus, see: Tochka, Сколько денег мошенники увели у белорусов, рассказали в Нацбанке, 28 October 2025, https://tochka.by/articles/economics/skolko_deneg_moshenniki_uveli_u_belorusov_rasskazali_v_natsbanke. Population estimates calculated as of December 2024.

91 See, for example, Sputnik Belarus, СК завершил расследование дела крупнейшей скам-группы Беларуси, 9 January 2024, https://sputnik.by/20240109/sk-zavershil-rassledovanie-dela-krupneyshey-skam-gruppy-belarusi-1082663006.html; Galina Puzyna, Крупную банду онлайн-мошенников задержали в Беларуси: в сутки она совершала до 30 краж, Mir24, 20 December 2022, https://mir24.tv/news/16535220/krupnuyu-bandu-onlain-moshennikov-zaderzhali-v-belarusi-v-sutki-ona-sovershala-do-30-krazh.

92 Alexander Lukashenko, Лукашенко: Жизнь нас подталкивает к этому! Преступный «колл-центр» в Минске, RTR-Belarus News, YouTube, 5 August 2025, 5:29, https://www.youtube.com/watch?v=utKNZcdT7hM&t=329s.

93 AI fraud reaches new level in Belarus, BelSat, 18 November 2025, https://en.belsat.eu/90080095/ai-fraud-reaches-new-level-in-belarus.

94 Kyrgyzstan: Mariia Indina, Thefts from bank cards are on the rise: Kyrgyz citizens have lost more than 15 million KGS in six months, Akchabar, 30 September 2024, https://www.akchabar.kg/en/article/ekonomika-fmluaeuoncqnjkhr/rost-krazh-s-bankovskikh-kart-za-polgoda-kirgizstantsi-poteryali-bolee-15-mln-somov-cvkqbgtmsfbqaprm; Ukraine: Interfax, Loss from fraudulent card transactions in 2024 increases by 37% while their number decreases by 1% – NBU, 12 May 2025, https://en.interfax.com.ua/news/economic/1071180.html; Russia: Fraudsters stole 27 billion rubles from Russians in 2024, *Izvestia*, 18 February 2025, https://en.iz.ru/en/1841157/2025-02-18/fraudsters-stole-27-billion-rubles-russians-2024; Belarus: Tochka, Сколько денег мошенники увели у белорусов, рассказали в Нацбанке, 28 October 2025, https://tochka.by/articles/economics/skolko_deneg_moshenniki_uveli_u_belorusov_rasskazali_v_natsbanke. Population estimates calculated as of December 2024.

95 Kazakhstan: Gulnar Nadirova, Digital security and threats in Kazakhstan, Eurasian Research Institute, 4 February 2025, https://www.eurasian-research.org/publication/digital-security-security-and-threats-in-kazakhstan; Fintech UZ, *Kiberfiribgarlik, xususan, bank kartalari bilan bog'liq jinoyatlar...*, Instagram, 31 October 2025, https://www.instagram.com/p/DQeVaHtDlBm. Uzbekistan: Ministry of Internal Affairs, Creating a safe cyberspace by combating cybercrime. Uzbekistan's experience in the early prevention of cybercrime in the context of digital transformation. Uzbekistan's experience in preventing cybercrime and ensuring a safe cyberspace, 7 May 2025, https://gov.uz/en/iiv/news/view/52319; Kyrgyzstan: Marina Onegina, The Ministry of Internal Affairs of the Kyrgyz Republic spoke about popular fraud schemes, 3 March 2026, https://open.kg/ky/news/local-news/77882-v-mvd-kr-rasskazali-o-populjarnyh-shemah-moshennichestva.html.

96 Akimat of the City of Astana, Астанада жыл басынан бері 2 алаяқтық колл-орталығы жойылды, Instagram, 15 December 2025, https://www.instagram.com/astana_akimdigi_akimat_astana/reel/DSSZufFCP3n; Aigerim Tarina, Қазақстандықтарды алдап келген алаяқтардың call-орталығы жойылды, Zakon, 4 April 2025, https://kaz.zakon.kz/kogam-tynysy/6059578-azastandytardy-aldap-kelgen-alayatardy-callortalyy-zhoyyldy.html.

97 Aigerim Tarina, Киберполицейлер 102 млн теңгеге интернет-алаяқтық ұйымдастырғандарды ұстады, Zakon.kz, 8 August 2025, https://kaz.zakon.kz/kogam-tynysy/6066016-kiberpolitseyler-102-mln-tegege-internetalayaty-yymdastyrandardy-stady.html.

98 Banks, В Бишкеке задержан гражданин Беларуси, подозреваемый в крупном мошенничестве, 6 June 2024, https://banks.kg/news/citizen-belarus-suspected-

major-fraud; Pozirk, Мингорсуд начал процесс над 55 участниками мошеннических “колл-центров”, 29 September 2025, https://pozirk.online/ru/news/157628.

99 Uz Daily, Fraud network targeting Russian citizens uncovered in Uzbekistan, 4 February 2025, https://www.uzdaily.uz/en/fraud-network-targeting-russian-citizens-uncovered-in-uzbekistan; Uz Daily, Criminal group stealing funds from citizens’ bank cards neutralized by Tashkent Police, 17 March 2025, https://www.uzdaily.uz/en/criminal-group-stealing-funds-from-citizens-bank-cards-neutralized-by-tashkent-police.

100 Interview with a Kazakh lawyer, December 2025, online.

101 Interview with a Kyrgyz journalist, November 2025, online.

102 Shugyla Turlybek, Қазақстан, Украина және Чехия полициясы интернет-алаяқтардың екі трансұлттық қылмыстық тобын жойды, Policia.Kz, 29 April 2024, https://polisia.kz/qazaqstan-ukraina-zhane-chehiya-politsiyasy-internet-alayaqtardyng-eki-transulttyq-qylmystyq-tobyn-zhojdy; Riza Turdakynyzy, Шетелдік интернет алаяқтардың алдауына түскен қазақстандықтар 5,8 млрд теңгеге кредит рәсімдеп, 7 млрд теңге шығынға батқан, Kursiv, 20 October 2023, https://kz.kursiv.media/kk/2023-10-20/rztq-internetalayaq.

103 Interview with a Kazakh lawyer, December 2025, online.

104 Asyl Arman, Алматыда шетелдік интернет-алаяқтарға көмектескен екі адам ұсталды, Azattyq Ruhy, 20 August 2025, https://azattyq-ruhy.kz/news/94573-almatyda-sheteldik-internet-alaiaktarga-komektesken-eki-adam-ustaldy; Forbes.kz, Интернет-алаяқтықтың 10-нан астам дерегіне қатысы бар шетелдік ұстады, 15 December 2022, https://forbes.kz/news/newsid_290925.

105 Interview with a Kazakh lawyer, December 2025, online.

106 Ruslan Gabbasov, Неліктен қазақстандық нөмірлерден алаяқтар қоңырау шалуды жалғастырып жатыр, Kazinform, 5 November 2025, https://kaz.inform.kz/news/nelkten-kazakstandik-nomrlerden-alayaktar-konirau-shaludi-zhalgastirip-zhatir-244501.

107 Daniyor Tukhsinov, Over 12 million cyberattacks recorded in Uzbekistan in 2024, 3 February 2025, https://kun.uz/en/news/2025/02/03/over-12-million-cyberattacks-recorded-in-uzbekistan-in-2024.

108 Daniyor Tukhsinov, Uzbekistan’s cybercrime crisis: How scammers steal millions and evade capture, Kun.uz, 12 March 2025, https://kun.uz/en/news/2025/03/12/uzbekistans-cybercrime-crisis-how-scammers-steal-millions-and-evade-capture.

109 Daniyor Tukhsinov, Over 12 million cyberattacks recorded in Uzbekistan in 2024, 3 February 2025, https://kun.uz/en/news/2025/02/03/over-12-million-cyberattacks-recorded-in-uzbekistan-in-2024.

110 Daniyor Tukhsinov, Uzbekistan’s cybercrime crisis: How scammers steal millions and evade capture, Kun.uz, 12 March 2025, https://kun.uz/en/news/2025/03/12/uzbekistans-cybercrime-crisis-how-scammers-steal-millions-and-evade-capture.

111 Kun.uz, Cybercrime cases surge elevenfold across Uzbekistan, 23 December 2025, https://m.kun.uz/en/news/2025/12/23/cybercrime-cases-surge-elevenfold-across-uzbekistan; on 95% of cybercrimes being connected to bank cards, see: Kun.uz, Uzbekistan sees 68-fold surge in cybercrime: Nearly 2 trillion UZS stolen in five years, 29 May 2025, https://monitor.kun.uz/en/news/2025/05/29/uzbekistan-sees-68-fold-surge-in-cybercrime-nearly-2-trillion-uzs-stolen-in-five-years.

112 24, Internet fraud: Kyrgyzstanis lost 826 million soms in 2025, 12 March 2026, https://24.kg/english/365723_Internet_fraud_Kyrgyzstanis_lost_826_million_soms_in_2025.

113 Freedom House, Freedom in the world 2025: Kyrgyzstan, https://freedomhouse.org/country/kyrgyzstan/freedom-world/2025; Human Rights Watch, Kyrgyzstan: Events of 2024, https://www.hrw.org/world-report/2025/country-chapters/kyrgyzstan.

114 Interview with a Kyrgyz journalist, November 2025, online.

115 Dana Omirgazy, National Bank: Kazakhstan’s cashless payments surpass 85% in 2024, *Astana Times*, 29 January 2025, https://astanatimes.com/2025/01/national-bank-kazakhstans-cashless-payments-surge-to-over-85-in-2024.

116 ‘Kazakhstan, Kyrgyzstan, and Uzbekistan report 89 to 93 percent general adoption rate [of smartphones].’ Farrukh Irnazarov, Youth and digital technology in Central Asia: A comparative analysis of Uzbekistan, Kazakhstan, Kyrgyzstan, and Tajikistan, Central Asia-Caucasus Institute & Silk Road Studies Program, 18 December 2025, https://www.silkroadstudies.org/publications/silkroad-papers-and-monographs/item/13572-youth-and-digital-technology-in-central-asia-a-comparative-analysis-of-uzbekistan-kazakhstan-kyrgyzstan-and-tajikistan.html.

117 Kun.uz, Cybersecurity experts warn of rising fraud linked to APK files on Telegram, 19 November 2025, https://kun.uz/en/news/2025/11/19/cybersecurity-experts-warn-of-rising-fraud-linked-to-apk-files-on-telegram.

118 Kun.uz, Fraudsters running over 200 fake ‘Alisher Usmanov promotion’ Telegram groups arrested, 15 February 2025, https://kun.uz/en/news/2025/02/15/fraudsters-running-over-200-fake-alisher-usmanov-promotion-telegram-groups-arrested.

119 An unusual form of pyramid scheme that is popular in Uzbekistan involves asking the ‘member’ to perform mundane daily tasks, like watching videos or reading books: Kun.uz, New financial scam in Uzbekistan swindles billions through fake book reading platform,20 May 2025, https://kun.uz/en/news/2025/05/20/new-financial-scam-in-uzbekistan-swindles-billions-through-fake-book-reading-platform; Kun.uz, Instagram post, https://www.instagram.com/reel/C_ADq59slQc.

120 A triangle scam involves a fraudster advertising an attractive product or commodity on Telegram. A buyer gets in touch, seeking to buy it, whereupon the fraudster directs them to pay a crypto trader (whom the fraudster has been corresponding with regarding a fiat-crypto exchange). The buyer pays the trader, the trader releases the crypto to the fraudster, and the buyer receives nothing.

121 See, among other cases: Kun.uz, Bilol's Motors director on trial for defrauding 48 customers in UZS 13 billion scheme, 26 July 2025, https://kun.uz/en/news/2025/07/26/bilols-motors-director-on-trial-for-defrauding-48-customers-in-uzs-13-billion-scheme; Kun.uz, Unlicensed developer in Tashkent defrauds dozens in apartment scam, 16 July 2025, https://kun.uz/en/news/2025/07/16/unlicensed-developer-in-tashkent-defrauds-dozens-in-apartment-scam; Kun.uz, ADWorld founder taken into custody following Kun.uz investigation, 21 August 2025, https://kun.uz/en/news/2025/08/21/adworld-founder-taken-into-custody-following-kunuz-investigation.

122 24Kg, Group supplying phone scammers with accounts, SIM cards detained in Kyrgyzstan, 24.kg, 3 February 2026, https://24.kg/english/360351_Group_supplying_phone_scammers_with_accounts_SIM_cards_detained_in_Kyrgyzstan.

123 Interview with an investigative journalist and lawyer in Tbilisi, Georgia, October 2025.

124 Interview with an MP, Kyiv, Ukraine, February 2025.

125 Interview with investigative journalists and a lawyer, Tbilisi, Georgia, October 2025.

126 Ilya Varlamov, Fraudsters: How Russians are being defrauded of billions | Prison call centres, offices in Ukraine, neural networks, the dark web, YouTube, 1 April 2025, timestamp approx. 29:50, https://www.youtube.com/watch?v=6dRA71QdSCY&t=2506s

127 Interview with investigative journalists, Tbilisi, Georgia, October 2025.

128 This restriction is not universally observed in Georgia, as fraudsters have been found guilty of deceiving US victims. Prosecution Service of Georgia, Based on the evidence presented by the prosecutor's office, the court found the defendants guilty of fraudulently acquiring a large amount of money, 29 September 2023, https://pog.gov.ge/news/prokuraturis-mier-wardgenili-mtkicebulebebis-safuZvelze-didi-odenobiT-Tanxis-motyuebiT-dauflebis-fa?lng=eng.

129 Interview with a Georgian cyber expert, January 2026, online.

130 Interview with a Georgian NGO, June 2025, online.

131 Interview with a Georgian cyber expert, December 2025, online.

132 Interview with Morgan Limited's lawyer, conducted by Georgian partners, 15 September 2025.

133 Morgan Limited, Incorporation document [Official corporate record], 22 October 2018; OCCRP, Web of call-center 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.

134 According to a Georgian former scammer, positions for 'sales operator' or 'call centre operator' are listed on Jobs.ge, and the true nature of the work is only revealed later. This is similar to Ukraine, where jobs for customer service managers or retention managers are listed on public job websites such as Robota.ua and Work.ua, along with listings on Telegram. See: Robin Fabbro, Georgian and German authorities raid 'scam' call centre, OC Media, 21 October 2021, https://oc-media.org/georgian-and-german-authorities-raid-scam-call-centre.

135 Interview with a journalist, June 2025, online.

136 Ibid.

137 Ibid.

138 Civil Georgia, Journalists expose global scam operating out of Tbilisi, 6 March 2025, https://civil.ge/archives/667514; written submission from investigative journalists based in Georgia.

139 Beso Namchavadze, Why does Georgia have low wages?, Forbes Georgia, 16 August 2023, https://forbes.ge/en/why-does-georgia-have-low-wages.

140 Information supplied by investigative journalists, December 2025, by email.

141 GI-TOC, Kyiv calling: The scam call centre phenomenon in Ukraine, forthcoming.

142 Interview with a journalist, June 2025, online; interview with investigative journalists, Tbilisi, Georgia, October 2025.

143 Interview with investigative journalists, Tbilisi, Georgia, October 2025.

144 Ibid.

145 UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, p 61, https://www.un-ilibrary.org/content/books/9789211542622; OCCRP, The phantom investor: How a wanted meth kingpin posed as a tycoon in Georgia, 21 January 2026, https://www.occrp.org/en/investigation/the-phantom-investor-how-a-wanted-meth-kingpin-posed-as-a-tycoon-in-georgia.

146 Simon Goodley et al, Deepfakes, cash and crypto: how call centre scammers duped 6,000 people, *The Guardian*, 5 March 2025, https://www.theguardian.com/money/2025/mar/05/deepfakes-cash-and-crypto-how-call-centre-scammers-duped-6000-people.

147 CivilNet, **Ավելի համոզիչ, ավելի վտանգավոր. հայերեն դիփֆեյքերի նոր ալիք**, 20 September 2025, https://www.civilnet.am/news/975383/.

148 CivilNet, **Փաշինյանի դիփֆեյքով խարդախություն. սոցցանցերում կեղծ տեսանյութ է շրջանառվում**, 10 June 2025, https://www.civilnet.am/news/955863; CivilNet, **Փաշինյանի դիփֆեյքը ռուսերենով ներդրումային հարթակ է գովազդում**, 6 October 2025, https://bit.ly/4q2HypF.

149 Interview with an NGO, June 2025, online.

150 CSTO, Attention! We are warning about a new fraud scheme, 6 September 2025, https://en.odkb-csto.org/news/news_odkb/vnimanie-preduprezhdaem-o-novoy-skheme-moshennichestva/#loaded

151 Opentools.ai, Meta unveils 'Meta Video Seal'to tackle menacing deepfakes, 13 December 2024, https://opentools.ai/news/meta-unveils-meta-video-seal-to-tackle-menacing-deepfakes; Meta Help Centre, Testing new ways to combat scams, https://www.meta.com/en-gb/help/policies/494835429957019.

152 Bhaskar Sharma, Meta under fire as fake AI war video gains over 700K views, Digit, 10 March 2026, https://www.digit.in/news/general/meta-under-fire-as-fake-ai-war-video-gains-over-700k-views.html.

153 Arka, Central bank chairman: Over 400 cases of bank fraud recorded in Armenia in Q1, 11 June 2025, https://arka.am/en/news/economy/central-bank-chairman-over-400-cases-of-bank-fraud-recorded-in-armenia-in-q1-.

154 Interview with an NGO, June 2025, online; Hetq, **Հայաստանում կիբեռհանցագործությամբ զբաղվող անդրազգային կազմակերպություն է բացահայտվել. ոստիկանություն**, 24 January 2024, https://www.hetq.am/hy/article/163747; Armenian Police, **Խուզարկություն զանգերի կենտրոնում. խարդախների թիրախում բացառապես օտարերկրացիներ էին**, 16 October 2024, https://www.police.am/news/view/qogv161024.html; Armenia Police, **Խարդախության միջոցով քաղաքացիներից գումար հափշտակելու նոր միջոց. ՆԳՆ ոստիկանությունը զգուշացնում է**, 28 August 2024, https://www.police.am/news/view/%D5%AD%D5%A1%D6%80%D5%A4%D5%A1%D5%AD280824.html; Shugyla Turlybek, МВД: Транснациональная преступная группа, занимавшаяся интернет-мошенничеством, задержана в Армении, Polisia.kz, 18 February 2025, https://polisia.kz/ru/mvd-transnatsional-naya-prestupnaya-gruppa-zanimavshayasya-internet-moshennichestvom-zaderzhana-v-armenii; Azat TV, **Հայաստանում կասեցվել է անօրինական զանգերի կենտրոնի գործունեություն. Ինչպես են խաբում ներդրողներին**, AzatTV, 10 February 2025, https://azat.tv/illegal-call-center-shut-down-armenia.

155 Interview with a journalist, Yerevan, Armenia, October 2025; interview with an NGO, June 2025, online.

156 Interview with an NGO, June 2025, online; Armenian Police, **Ի՞նչ է ֆիշինգը: ՀՀ-ում տարածում գտած նոր ձևը**, 19 May 2025, https://www.police.am/news/view/%D6%86%D5%AB%D5%B7%D5%AB%D5%B6%D5%A3190523.html; NewsAm, **Հեռախոսային խարդախության նոր ձև է տարածվում. ինչպե՞ս խաբեության զոհ չդառնալ**, 29 April 2025, https://news.am/arm/news/880181.html.

157 How2B, **Զեղծարարների կողմից անձնական և բանկային տվյալներ ձեռք բերելու փորձերն ավելացել են. ԿԲ**, 9 August 2024, https://how2b.am/fraudsters-attempts-to-obtain-banking-info-have-increased.

158 How2B, 28.3 **մլն դրամ՝ 7 օրում. խարդախության նոր մեթոդ՝ թիրախում մեծահասակներն են**, 13 August 2024, https://how2b.am/elderly-are-targeted-by-scammers.

159 The average Armenian monthly salary in 2024 was 287 172 Armenian drams. CEIC Data, Armenia average monthly nominal wage: Annual, https://www.ceicdata.com/en/armenia/average-monthly-real-and-nominal-wages/average-monthly-nominal-wage-annual.

160 Shugyla Turlybek, МВД: Транснациональная преступная группа, занимавшаяся интернет-мошенничеством, задержана в Армении, Polisia.kz, 18 February 2025, https://polisia.kz/ru/mvd-transnatsional-naya-prestupnaya-gruppa-zanimavshayasya-internet-moshennichestvom-zaderzhana-v-armenii.

161 Armenpress, Watch: Armenian special police units raid fake call center running international scam, 25 November 2025, https://armenpress.am/en/article/1235895.

162 Interview with a Georgian cybercrime expert, January 2026, online.

163 Interview with an NGO, June 2025, online; Arka Telecom, Phishing and 'romance' scams: cybercrime on the rise in Armenia, 6 March 2025, https://arkatelecom.am/en/news/telecom/-phishing-and-romance-scams-cybercrime-on-the-rise-in-armenia.

164 Interview with an NGO, June 2025, online.

165 Interview with a former World Bank employee, Yerevan, Armenia, October 2025.

166 Oimaq, Алматыда алаяқтық жасаған шетелдік азамат анықталды, 30 January 2025, https://oimaqnews.kz/2507/almatyda-alaya-ty-zhasa-an-sheteldik-azamat-any-taldy; Umitkul Nur, Қазақстанға интернет-алаяқтық жасау мақсатында келген шетелдік азамат тұтқындалды, Polisia.kz, 20 February 2025, https://polisia.kz/qazaqstangha-internet-alayaqtyq-zhasau-maqsatynda-kelgen-sheteldik-azamat-tutqyndaldy; Stanislav Doroshchenok, Из Алтая в Минск за чужими деньгами — правоохранители с поличным задержали двух курьеров телефонных мошенников, SB.by, 3 December 2025, https://www.sb.by/articles/iz-altaya-v-minsk-za-chuzhimi-dengami-zaderzhany-kurery-telefonnykh-moshennikov.html; BelTA, Обналичивали деньги обманутых пенсионеров. Задержаны двое пособников аферистов, 28 November 2025, https://belta.by/society/view/obnalichivali-dengi-obmanutyh-pensionerov-zaderzhany-dvoe-posobnikov-aferistov-751331-2025.

167 OCCRP, Suspected German scammer arrested in Georgia on extradition order, 4 November 2025, https://www.occrp.org/en/news/suspected-german-scammer-arrested-in-georgia-on-extradition-order.

168 Galina Khomulak, Орудуют "под носом" налоговой: на Печерске разоблачили колл-центр с турецкими

сотрудниками, StopCor, 7 November 2025, https://www.stopcor.org/section-uanews/news-oruduyut-pid-nosom-podatkovoi-na-pechersku-vikrili-kol-tsentr-iz-turetskimi-spivrobitnikami-07-11-2025.html.

169 General Prosecutor's Office (Ukraine), A transnational criminal organization that defrauded Czech citizens through a network of fraudulent call centres has been dismantled, 23 July 2025, https://gp.gov.ua/ua/posts/likvidovano-transnacionalnu-zlocinnu-organizaciyu-yaka-osukuvala-gromadyan-cexiyi-cerez-merezu-saxraiskix-kol-centriv.

170 Sonia Grad, У Франківську викрили шахрайський call-центр, який обікрав громадян ЄС на 50 мільйонів (ФОТО, ВІДЕО), Galka, 16 December 2025, https://galka.if.ua/u-frankivsku-vykryly-shakhrayskyy-call-tsentr-iakyy-obikrav-hromadian-yes-na-50-milyoniv-foto-video.

171 Shugyla Turlybek, Ministry of Internal Affairs: A transnational criminal group involved in online fraud has been detained in Armenia, Polisia.kz, 18 February 2025, https://polisia.kz/ru/mvd-transnatsional-naya-prestupnaya-gruppa-zanimavshayasya-internet-moshennichestvom-zaderzhana-v-armenii.

172 For example, the call centres shut down in Moscow in 20204 were staffed by people from 10 countries, but the countries were not named. *Kommersant*, В Москве раскрыты колл-центры, похитившие миллионы у граждан больше 20 стран, 11 December 2024, https://www.kommersant.ru/doc/7364335.

173 Alexey Ayriyan, Россиян предупредили о риске попасть в рабство в одной азиатской стране, URA.ru, 12 October 2025, https://ura.news/news/1053009624; UzReport, *Tailand ikki nafar firibgarlik qurboni bo'lgan O'zbekiston fuqarolarini vatanga qaytarishga yordam berdi*, 2 May 2025, https://uzreport.news/society/tailand-ikki-nafar-firibgarlik-qurboni-bo-lgan-o-zbekiston-fuqarolarini-vatanga-qaytarishg.

174 See, for instance, Liam O'Shea, Shadow states: High-level corruption and state capture in the South Caucasus, GI-TOC, August 2025, https://globalinitiative.net/analysis/high-level-corruption-and-state-capture-in-the-south-caucasus.

175 Radio Free Europe/Radio Liberty, Georgians keep up protest despite attacks against rally day before, 10 September 2025, https://www.rferl.org/a/georgia-demonstration-protesters-elections-georgian-dream/33526076.html.

176 Interview with an NGO, June 2025, online.

177 For example, Interfax, Омские экс-полицейские осуждены за организацию заработка на "крышевании" сутенеров, 22 March 2017, https://www.interfax-russia.ru/siberia/news/omskie-eks-policeyskie-osuzhdeny-za-organizaciyu-zarabotka-na-kryshevanii-sutenerov; Daria Grigorenko, В Ленобласти разоблачили полицейских, продававших покровительство коммерсантам, VZ, 10 July 2025, https://vz.ru/news/2025/7/10/1344415.html; Delovoy Peterburg, Майора полиции лишили звания и посадили на 12 лет за крышевание обнальщиков, 23 December 2024, https://www.dp.ru/a/2024/12/23/majora-policii-lishili-zvanija.

178 GI-TOC, Kyiv calling: The scam call centre phenomenon in Ukraine, forthcoming.

179 Interview with an NGO, June 2025, online.

180 Interview with a Western diplomat, Tbilisi, Georgia, October 2025.

181 Interview with a Georgian cybersecurity expert, December 2025.

182 Interview with a lawyer, Tbilisi, Georgia, October 2025.

183 Interview with a lawyer, Tbilisi, Georgia, October 2025; Civil Georgia, Amnesty International: Georgian government greenlights violence against its critics, 12 June 2024, https://civil.ge/archives/612498; BNE IntelliNews, Masked 'titushky' thugs target journalists and opposition members in Tbilisi, 8 December 2024, https://www.intellinews.com/masked-titushky-thugs-target-journalists-and-opposition-members-in-tbilisi-357255.

184 Interviews with investigative journalists and a lawyer, October 2025.

185 According to the interviewee, 'The old government guys under investigation were the ones running the call centres' operation.' Interview with a diplomat, Tbilisi, Georgia, October 2025. OCCRP, Georgia detains ex-security chief over alleged bribes tied to global scam call centers, 23 December 2025, https://www.occrp.org/en/news/georgia-detains-ex-security-chief-over-alleged-bribes-tied-to-global-scam-call-centers.

186 Rayhan Demytrie, Spectacular downfall of Georgia's ex-PM accused of having $6.5m in his flat, BBC, 24 October 2025, https://www.bbc.com/news/articles/cjekw5jxw89o; Ex-Prime Minister Garibashvili to serve five years in prison after plea deal, Civil.ge, 12 January 2026, https://civil.ge/archives/717027.

187 Mikheil Gvadzabia, Georgian journalist Eliso Kiladze among 10 charged with fraud and money laundering, 18 February 2026, https://oc-media.org/georgian-journalist-eliso-kiladze-among-10-charged-with-fraud-and-money-laundering.

188 Interview with a lawyer, Tbilisi, Georgia, October 2025.

189 Interview with a Georgian cyber expert, December 2025.

190 Interview with a lawyer, Tbilisi, Georgia, October 2025.

191 Prosecutor's Office of Georgia, **საქართველო ს პროკურატურამ … გახსნა**, 6 September 2024, https://pog.gov.ge/news/saqarTvelos-prokuraturam-germaniis-federaciuli-respublikis-samarTaldamcavebTan-TanamshromlobiT-qol.

192 Tbilisi City Court, Verdict of Tbilisi City Court [unpublished official document], 27 June 2025.

193 Ibid.

194 Financial Police of Georgia, Financial Police raid at Morgan Limited LLC [unpublished official document], 2019; G

Meshveliani, Search protocol [unpublished official document]. 17 December 2019.

195 Mtavari Arkhi, ნიკა გვარამიას ექსკლუზიური ინტერვიუ | ე.წ. ქოლცენტრების სქემის სრული ანატომია, YouTube, 9 April 2022, https://www.youtube.com/watch?v=mmXTggq1Mbw&t=431s.

196 Ibid.

197 Tbilisi City Court, Decision on freezing assets, 23 January 2023; Tbilisi City Court. Decision on freezing assets 18 January 2024; Tbilisi City Court, Decision on freezing assets, 16 January 2025.

198 Interview with a lawyer, Tbilisi, Georgia, October 2025.

199 On Ukrainian conflict-related scams, see GI-TOC, Kyiv calling: The scam call centre phenomenon in Ukraine, forthcoming. On Russian conflict-related scam: F6, «Получите миллион»: мошенники создали более 500 сайтов фейкового фонда поддержки участников СВО, 24 November 2025, https://www.f6.ru/media-center/press-releases/investscam-svo.

200 Ivan Zhadaev, «Охота на «мамонтов». Как работают украинские мошенники, Verstka, 1 December 2025, https://verstka.media/kak-rabotayut-ukrainskie-moshenniki.

201 Interview with a Western law enforcement liaison, November 2025, online.

202 Written communication with a Ukrainian scammer, December 2025.

203 Mihir Bagwe, Ukraine cracks down on investment scams, raids call centers, Bank Security Info, 27 June 2023, https://www.bankinfosecurity.com/ukraine-cracks-down-on-investment-scams-raids-call-centers-a-22386.

204 Julia Shramko, "Від слів до справ": Кравченко повідомив про викриття у межах міжнародної співпраці схеми наживи шахраїв на громадянах ЄС на близько $250 тисяч, UNN, 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.

205 *Izvestia*, Channel without communication: Sanctions against Russia slow down the investigation of crimes in the EU, 6 February 2025, https://en.iz.ru/en/node/1895848.

206 Styopa Net, Милтон групп - Индустрия обмана, YouTube, 17 December 2024, https://www.youtube.com/watch?v=bGkBRaYffd4.

207 Scott Anderson, How Georgia went from the vanguard of democracy to the front lines of autocracy, *The New York Times*, 20 August 2025, https://www.nytimes.com/2025/08/20/magazine/georgia-russia-autocracy-dictatorship.html.

208 Rikard Jozwiak, EU calls Georgia candidate 'in name only' after backsliding on reforms, RFE/RL, 4 November 2025, https://www.rferl.org/a/eu-georgia-candidate-backsliding-reforms-ukraine-moldova-serbia/33581352.html.

209 Lucy Papachristou, 'Five minutes away from one-party dictatorship': Georgia's U-turn from Western path, Reuters, 18 November 2025, https://www.reuters.com/world/five-minutes-autocracy-how-georgia-u-turned-its-western-path-2025-11-18.

210 Rayhan Demytrie and Emily Atkinson, Georgia approves controversial 'foreign agent' law, sparking more protests, BBC, 14 May 2024, https://www.bbc.co.uk/news/world-europe-69007465; Nini Gabritchidze, Georgian Dream's FARA takes effect, Civil Georgia, 31 May 2025, https://civil.ge/archives/684669; interviews with investigative journalists, Tbilisi, Georgia, October 2025.

211 Interview with a Western diplomat, Tbilisi, Georgia, October 2025.

212 Interview with a Western law enforcement official, Tbilisi, Georgia, October 2025.

213 Interview with journalist, Tbilisi, Georgia, October 2025.

214 In the aftermath of the full-scale invasion, INTERPOL directed that all diffusions from Moscow would have to be sent to the General Secretariat, not member branches, to check for compliance with INTERPOL's rules. In Russia, INTERPOL has been cast as refusing to cooperate. Ukraine: INTERPOL General Secretariat statement, 10 March 2022, https://www.interpol.int/News-and-Events/News/2022/Ukraine-INTERPOL-General-Secretariat-statement; TASS, Interpol not cooperating with Russia after launch of special op — Investigative Committee, 13 December 2024, https://tass.com/politics/1886903.

215 BBC, Russia using Interpol's wanted list to target critics abroad, leak reveals, 26 January 2026, https://www.bbc.co.uk/news/articles/c20gg729y1yo; Russia's Interior Ministry limits Interpol powers in country, *Novaya Gazeta*, 18 August 2023, https://novayagazeta.eu/articles/2023/08/18/russias-interior-ministry-limits-interpol-powers-in-country-en-news.

216 BBC, Moscow attack: Russia blames West and Kyiv for jihadist massacre, 26 March 2024, https://www.bbc.co.uk/news/world-europe-68663043.

217 Interview with a Western law enforcement liaison, November 2025, online.

218 Ibid.

219 On Russia, Belarus, Kazakhstan and Uzbekistan cooperation, see: BelTA, The situation was turned around. For the first time in recent years, the Ministry of Internal Affairs records a decrease in cybercrime, 5 November 2025, https://belta.by/society/view/situatsiju-udalos-perelomit-mvd-vpervye-za-poslednie-gody-fiksiruet-snizhenie-kiberprestuplenij-747107-2025/; BelTA, Law enforcement officers of Belarus and Russia have planned joint steps to suppress cybercrime, 21 November 2025, https://belta.by/society/view/pravoohraniteli-belarusi-i-rossii-splanirovali-sovmestnye-shagi-po-presecheniju-kiberprestuplenij-750117-2025; On Kyrgyzstan regional cooperation, see case of Belarusian national cited in Central Asia section.

220 Interview with a Georgian cybercrime expert, January 2025. On 9 months maximum pre-trial detention, see Georgian Criminal Procedure Code 1998 (2024), Article 205, 2, https://cjad.nottingham.ac.uk/en/legislation/1684/keyword/755.

221 Interview with a Georgian cybercrime expert, January 2025.

222 Ibid.

223 Netzpolitik, An automated fraud machine, 16 October 2025, https://netzpolitik.org/2025/angebliche-online-investments-eine-automatisierte-betrugsmaschine.

224 Jeff Horwitz, Meta is earning a fortune on a deluge of fraudulent ads, documents show, 6 November 2025, https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06.

225 Both Kazkahstan and Uzbekistan implemented 'anti-spoofing' measures in 2025. Mobile operators in Kazakhstan are now required to use anti-fraud systems and report suspected fraud activity to the National Bak's anti-fraud centre. EL.kz, Kazakhstan to block scam phone numbers, 18 November 2025, https://el.kz/en/kazakhstan-to-block-scam-phone-numbers_400040763; Kun.uz, Mobile operators start blocking fake-number calls in Uzbekistan, 22 October 2025, https://kun.uz/en/news/2025/10/22/mobile-operators-start-blocking-fake-number-calls-in-uzbekistan.

226 Interfax, State Duma passes law to combat telephone fraud, Interfax, 25 March 2025, https://interfax.com/newsroom/top-stories/110583; Bank of Russia, New methods to protect people against fraudulent transactions, 24 July 2024, https://www.cbr.ru/eng/press/event/?id=18866.

227 TASS, Sberbank's deputy chairman called for tougher penalties for deepfake fraud, 18 November 2025, https://tass.ru/ekonomika/25658169.

228 *Izvestia*, Antifrod system prevented 33 mln calls from spoofed numbers in January, 21 February 2025, https://en.iz.ru/en/1843044/2025-02-21/antifrod-system-prevented-33-mln-calls-spoofed-numbers-january.

229 John Haraburda, What is SIM box fraud: Understanding telecoms' most challenging scam, TSN, 5 August 2025, https://tnsi.com/resource/com/what-is-sim-boxing-blog. On specific cases, see, for example, Vesiskitim, A GSM fraud ring was uncovered in Novosibirsk: call centers were set up in rented apartments, 1 October 2025, https://vesiskitim.ru/2025/10/01/v-novosibirske-raskryli-set-gsm-moshennikov-call-tsentry-obustroili-v-semnyh-kvartirah.

230 Naša Niva, Four Minsk women were arrested for assisting telephone scammers. They installed special equipment at home, 1 December 2025, https://nashaniva.com/en/382531.

231 Yana Chernikova and Polina Lvova, Communications under control: How the new SIM card registration and verification procedure will work, *Izvestia*, 29 October 2025, https://iz.ru/1980384/ana-cernikova-polina-lvova/svaz-pod-kontrolem-kak-budet-rabotat-novyi-poradok-oformlenia-i-verifikacii-sim-kart. On duplicate SIM scams: RBC, The Ministry of Internal Affairs has warned of a fraudulent scheme involving the copying of Russian SIM cards, 10 October 2025, https://www.rbc.ru/life/news/68e8afa49a794726cdfad375.

232 Mediazona, No country for calls. Russian censorship agency confirms throttling voice calls on WhatsApp and Telegram to "fight crime", 13 August 2025, https://en.zona.media/article/2025/08/13/callban.

233 RBC, Sberbank warned of the risk of Max account theft, 4 September 2025, https://www.rbc.ru/rbcfreenews/68b973039a7947a6b118c36b; Oleg Loginov, Max by default: Russia makes state messenger mandatory, 2 September 2025, https://www.dw.com/ru/max-po-umolcaniu-rossia-delaet-gosmessendzer-obazatelnym/a-73853829.

234 Reporters Without Borders, In Ukraine's occupied territories, the Kremlin's messaging app Max is building a digital Iron Curtain, no date, https://rsf.org/en/ukraine-s-occupied-territories-kremlin-s-messaging-app-max-building-digital-iron-curtain; Anastasia Gavrilyuk, Keep the deception wider: How authorities fought fraudsters in 2025, Forbes, 6 January 2026, https://www.forbes.ru/tekhnologii/552363-derzi-obman-sire-kak-vlasti-borolis-s-mosennikami-v-2025-godu.

235 Sergey Kagermazov and Svetlana Reiter, Russia's WeChat: What's known about Max, the messenger app that could replace WhatsApp?, BBC, 21 July 2025, https://www.bbc.com/russian/articles/cn419l9k7wno.

236 See, for example, this piece in *Rossiyskaya Gazeta*, a state-controlled media outlet. Oleg Kapranov and Anastasia Kalenitskaya, Surveillance, hackers, and sneaky AI: experts examine the most popular horror stories about the national messaging app MAX, *Rossiyskaya Gazeta*, 28 September 2025, https://rg.ru/2025/09/25/odnim-maxom.html. See also: Andrey Zaytsev, 'The messenger that will spy on us': Debunking the most ridiculous myths about the MAX app, *Komsomolskaya Pravda*, 6 September 2025, https://www.kp.ru/daily/27748.5/5138878.

237 Interview with a Western diplomat, Tbilisi, Georgia, October 2025.

238 TASS, Sberbank Deputy Chairman Kuznetsov: Telephone fraud statistics have failed to reverse, 18 November 2025, https://tass.ru/ekonomika/25657123.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with 800 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