

**Transnational Crime Networks Originating in Georgia: Scammer Call
Centers**

Levan Tsirgvava

August 2023,

**Rondeli Foundation: Georgian Foundation for Strategic and
International Studies, Tbilisi**

Introduction

After the end of the Cold War, scholars have suggested expanding the definition of national security¹. Previously, international security studies were military-centered; however, with greater attention directed towards the threats of environmental degradation, economic disparities, chronic poverty, food security, diseases such as HIV/AIDS, transnational crime, and international migration after the Cold War², military confrontation is no longer the sole means for states to address security threats. Global crime networks pose significant security threat due to their ability to operate across borders, engage in diverse illicit activities, and undermine the stability and well-being of nations. With humanity entering the era of the fourth industrial revolution, characterized by interconnectedness, new opportunities have emerged for criminals to exploit, such as fraud, which has become an increasing security threat. This is evidenced by the UK government's initiative to reclassify fraud as a national security threat, thereby elevating fraud to the same level of threat as terrorism³. Recently, Georgia has become a hub for scammer call centers that target EU citizens as their victims. The vast scale of the call centers indicates the presence of a strong hierarchical system managing them. This essay will firstly give a general overview of what fraud and scammers are and then it will move on to examine the operations of these criminal networks, in Georgia, analyze the political dynamics surrounding them, and explore the implications they can have for Georgia's aspirations to become a member state of the EU.

What is Fraud and who are Scammers?

Firstly, it is necessary to define fraud and understand how fraud call centers function. According to EU Serious and Organized Crime Threat Assessment (SOCTA) report, fraud is when individuals purposely deceive others through dishonest means, aiming to gain an

¹ Dannreuther, Roland. 2013. *International Security : The Contemporary Agenda*. Oxford: Polity Press. Page 20

² Ibid

³ Cameron, Sarah, and Sarah Cameron. 2023. "Fraud to Be Reclassified as a UK National Security Threat." *ComplyAdvantage*, February. <https://complyadvantage.com/insights/fraud-to-be-reclassified-as-a-uk-national-security-threat>.

unfair advantage or cause harm⁴. These acts involve the intentional and deceptive manipulation of information, leading to the voluntary but illegal transfer of assets, goods, or undeserved benefits to the perpetrators⁵. Criminals are capitalizing on the digital era, leveraging fraudulent activities to their advantage. As a result, multiple forms of fraud have emerged. Phishing schemes, credit card fraud, identity theft, and investment fraud are examples of these. Phishing schemes include duping people into disclosing personal information, whereas credit card theft involves unauthorized transactions using stolen card information. Identity theft happens when someone's personal information is utilized without their permission. Furthermore, investment fraud is tricking individuals with inaccurate or misleading information, which can result in significant financial losses⁶. One concerning aspect of these frauds is their ease of execution. They can be committed without any physical contact between the victim and the perpetrator; everything takes place within the digital realm. Fraudsters employ sophisticated techniques, manipulating strangers through phone calls. Exploiting either the victims' limited internet knowledge or by gaining their trust, they manipulate individuals into divulging personal information or unknowingly participating in deceptive schemes, such as fake investments. These techniques adopted by scammers is called cold calling⁷. Call centers are made up of multiple cold callers working in an office setting, making a large number of calls each day with the intention of scamming as many people as they can.

Scholars have suggested that policies targeted at limiting internet fraud should consider that victims of internet fraud are diverse, with no one specific demographic being exclusively affected⁸. However, it can be argued that a particular demographic is still more commonly victimized by internet fraud. According to scholar Cohen, senior individuals

⁴“Serious and Organised Crime in the EU: A Corrupting Influence,” Europol, n.d., <https://www.europol.europa.eu/media-press/newsroom/news/serious-and-organised-crime-in-eu-corrupting-influence>.

⁵ “Serious and Organised Crime in the EU: A Corrupting Influence,” Europol, n.d., <https://www.europol.europa.eu/media-press/newsroom/news/serious-and-organised-crime-in-eu-corrupting-influence>.

⁶ Ibid

⁷ Ibid

⁸ Norris, Gareth, Alexandra Brookes, and David Dowell. 2019. “The Psychology of Internet Fraud Victimization: A Systematic Review.” *Journal of Police and Criminal Psychology* 34 (3): 231–45. <https://doi.org/10.1007/s11896-019-09334-5>.

often display remarkable generosity when it comes to charitable contributions. However, they may lack awareness that fraud constitutes a crime, leading them to overlook their victimization and refrain from reporting it to the authorities⁹. Additionally, they might feel embarrassed and thus hesitate to seek the necessary support or treatment¹⁰.

Furthermore, cold callers employ sophisticated psychological techniques to influence their victims. Persuading people to invest their own money is not easy. Thus, scammers have developed multiple techniques, which are written in their guidelines. As the study of the United States Justice Department points out social psychology is for understanding how to tackle internet fraud. Social psychology, particularly focusing on the psychology of persuasion, offers valuable insights into internet fraud dynamics. There are three main aspects to consider¹¹. Firstly, the alternative routes to persuasion involve the central route with logical arguments and deep thinking, and the peripheral route with emotional triggers and shortcuts for quick acceptance. Fraudsters frequently resort to peripheral routes, triggering strong emotions and distracting victims from logical thinking to exploit deceptive tactics successfully¹². Secondly, internet fraud involves a discrepancy between victims' beliefs and criminals' attitudes, with victims mistakenly assuming a shared expectation of value exchange while criminals are fully aware of the deception¹³. Moreover, fraudsters may use derogatory terms to refer to victims, minimizing empathy and facilitating the delivery of false representations¹⁴. Lastly, social psychology identifies persuasive techniques like authority, scarcity, liking and similarity, reciprocation, and consistency, which fraudsters employ to manipulate victims effectively¹⁵. The high level of sophistication exhibited by scammers results in numerous people falling prey to their

⁹ Cohen, Carole. 2006. "Consumer Fraud and the Elderly." *Journal of Gerontological Social Work* 46 (3-4): 137-44. https://doi.org/10.1300/j083v46n03_08.

¹⁰ Ibid

¹¹ Rusch, Jonathan J. 2003. "The 'Social Engineering' of Internet Fraud." *United States Justice Department*, January. <http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf>. Page 3-5

¹² Ibid

¹³ Rusch, Jonathan J. 2003. "The 'Social Engineering' of Internet Fraud." *United States Justice Department*, January. <http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf>.

¹⁴ Ibid

¹⁵ Ibid

schemes, underscoring the significance of implementing policies aimed at eradicating scammer call centers. However, it also highlights the challenges and complexities involved in tackling this issue.

Case of Georgia

In recent years, scammer call centers have significantly multiplied in Georgia, attracting attention from Georgia's European allies due to their citizens falling prey to fake investment schemes. In 2023, BBC reporter Simina Weinglass conducted an extensive investigation on call centers originating in Georgia, revealing that they had collectively scammed over a billion dollars¹⁶. Their investigation was remarkably thorough, shedding light on the intricate workings of these call centers, their origins, and the methods they employ to victimize people. They identified one of the scammer companies named "The Milton Group," which was originally named by the scammers themselves but abandoned in 2020. According to their investigation, a total of 152 brands are believed to be part of this network. Their modus operandi involves focusing on investors and swindling them out of significant sums, ranging from thousands to hundreds of thousands of pounds. Interestingly, one of the investment brands associated with the Milton Group went as far as sponsoring a top-tier Spanish football club and advertising in major newspapers, bolstering its credibility and attractiveness to potential investors¹⁷. The remarkable growth of these transnational scammer companies, originating in Georgia and extending their reach to top-tier football clubs in major leagues, underscores their high level of sophistication. It exemplifies how, with the aid of new technologies, criminal organizations from anywhere in the world can effortlessly connect with audiences in the heart of Europe - making it difficult for policymakers to challenge them.

Additionally, the BBC's report showed important insights into how exactly the scammers contact their victims and how they persuade them into investing into fake trading platforms. Based on their report, many victims are enticed by social media ads and sign

¹⁶ Gunter, By Max Hudson Simona Weinglass, Mark Turner and Joel. 2023. "On the Hunt for the Businessmen behind a Billion-Dollar Scam." *BBC News*, April 11, 2023. <https://www.bbc.com/news/world-65038949>.

¹⁷ Ibid

up quickly. Within 48 hours, they receive a phone call promising high returns of up to 90% per day. These calls are typically made from seemingly legitimate call centers with professional setups, complete with HR departments, targets, bonuses, and competitions. However, they also employ unethical practices, guiding victims on exploiting investors' weaknesses. Victims can end up with regulated or unregulated companies, with some being pushed towards high-risk trades leading to losses. Others are instructed to download software for remote control of their PCs, allowing scammers to trade on their behalf. Former employees reveal that some victims believe they are making real trades, but their money is merely being siphoned away¹⁸. These findings suggest the existence of a robust and well-established company that has undergone significant development over an extended period, thriving despite operating under constraints and limitations by law.

The BBC's investigation sheds light on a captivating aspect related to the strategic targeting of fraudsters towards specific demographics. Notably, in Canada, a substantial portion of fraud victims consists of elderly individuals¹⁹. Similarly, this trend finds parallels in the context of victims falling victim to Georgian scammer call centers. Victims of fraud investigated by in the BBC's report are mostly the elderly. For example, Jan Erik, a 75-year-old retiree living in Sweden, who finds himself on the verge of falling victim to yet another scam²⁰. His vulnerability and the distressing loss he has experienced highlight the pervasive issue of financial exploitation targeting elderly individuals like Jan Erik.

The BBC report was published in the year 2023. However, the severity of the call center issue in Georgia had already become apparent earlier. In 2021, according to data from the Prosecutor's Office, a total of 18 individuals were arrested as part of an ongoing investigation into the call center schemes²¹. Then, in 2022, the Finance Minister of

¹⁸ Gunter, By Max Hudson Simona Weinglass, Mark Turner and Joel. 2023. "On the Hunt for the Businessmen behind a Billion-Dollar Scam." *BBC News*, April 11, 2023. <https://www.bbc.com/news/world-65038949>.

¹⁹ Cohen, Carole. 2006. "Consumer Fraud and the Elderly." *Journal of Gerontological Social Work* 46 (3-4): 137-44. https://doi.org/10.1300/j083v46n03_08.

²⁰ Gunter, By Max Hudson Simona Weinglass, Mark Turner and Joel. 2023. "On the Hunt for the Businessmen behind a Billion-Dollar Scam." *BBC News*, April 11, 2023. <https://www.bbc.com/news/world-65038949>.

²¹ Civil.Ge. 2022. "Five Arrested in Alleged International Fraud Scheme." *Civil Georgia*, February 18, 2022. <https://civil.ge/archives/473660>.

Georgia, Lasha Khutsishvili, announced the closure of 46 call center companies due to the finance ministry's investigation into alleged criminal activities²². These incidents underscore the longstanding nature of the problem and the authorities' efforts to address it. However, it also implies that the efforts put into eliminating the scammer call centers, in Georgia, have not been enough. The issue persists. The persistent nature of the issue may be attributed to two primary factors. Firstly, the considerable level of sophistication displayed by these companies in concealing their illegal activities could pose significant challenges to law enforcement efforts. Secondly, the existence of an enabling environment that fosters their growth and prosperity raises concerns about potential involvement of high-level figures in corrupt practices.

Most importantly, the political twist that revolves around the Georgian scammer companies is regarding the question who owns these companies and who profit from it. The government of Georgia and its opposition have engaged in a continuous back-and-forth exchange, each attributing blame to the other regarding the responsibility for the presence and actions of the scammer companies. The scammer companies that the BBC investigated, according to them, are linked to Georgia's former Minister of Defense, Davit Kezerashvili²³, who is currently the owner of the major opposition Tv channel- Formula Tv. On the other hand, one of the opposition leaders, Levan Khabeishvili, has repeatedly accused Grigol Liluashvili, the head of Georgia's State Security Service, of shielding and benefiting from the purported international scam, alongside Ucha Mamatsashvili, a relative of the Georgian Dream founder billionaire Bidzina Ivanishvili²⁴. Khabeishvili also asserted that the government used the profits to bribe individuals for the pre-election period and voting days²⁵. The two different narratives create the image as if all of the fraudulent companies are the responsibility of either the government or the opposition. However, one narrative does not necessarily exclude the other. A person named Giorgi,

²² "Finance Minister: 46 Call Centres Operating in Georgia under Investigation for Alleged Illegal Activities." n.d. Agenda.Ge. <https://agenda.ge/en/news/2022/1222>.

²³ Gunter, By Max Hudson Simona Weinglass, Mark Turner and Joel. 2023. "On the Hunt for the Businessmen behind a Billion-Dollar Scam." *BBC News*, April 11, 2023. <https://www.bbc.com/news/world-65038949>.

²⁴ Civil.Ge. 2022. "Five Arrested in Alleged International Fraud Scheme." *Civil Georgia*, February 18, 2022. <https://civil.ge/archives/473660>.

²⁵ Ibid

who had worked in one of the scammer companies, states, "This business is not exactly undercover. I find it hard to imagine that the police didn't know about it."²⁶ Giorgi makes an interesting observation that this scale of illegal activity can't be unnoticed by the country's law enforcements. Thus, a same question arises how and who protects these companies. Considering that corruption is an integral element of almost every organized crime activity,²⁷ it can be argued that despite the high levels of animosity between Georgia's ruling party and the opposition, some officials and opposition leaders find common ground in their shared interest of generating money to fund political campaigns. This has led them to a mutual interest in profiting from this illegal activity. However, it has to be noted that, at this point, there is no proof which supports this thesis.

The transnational illegal activities discussed in the essay have not been unnoticed by Georgia's European allies. According to Eurasianet call-center fraud has emerged as a significant concern for Georgia and its interactions with European Union partners. According to various European diplomats who spoke to Eurasianet anonymously, European embassies have raised this matter with the Georgian authorities²⁸. This poses a significant challenge to Georgia's ambitions to become a EU member state. From the EU's standpoint Georgia is the origin of transnational fraud, which poses a significant human security threat as it preys on vulnerable individuals and communities, leading to devastating financial losses and psychological distress of their citizens. To tackle the issue of internet fraud Europol and Eurojust established joint forces. In January 2023, Eurojust provided assistance to law enforcement efforts by creating a collaborative investigative team to examine the online fraud scheme²⁹. Additionally, two specialized coordination meetings were organized to prepare for upcoming actions. Eurojust played a crucial role in facilitating the execution of European Arrest Warrants, European

²⁶ Lomsadze, Giorgi. 2022. "Scam Call Centers Proliferate in Georgia." *Eurasianet*, June. <https://eurasianet.org/scam-call-centers-proliferate-in-georgia>.

²⁷ "Serious and Organised Crime in the EU: A Corrupting Influence," Europol, n.d., p.26, <https://www.europol.europa.eu/media-press/newsroom/news/serious-and-organised-crime-in-eu-corrupting-influence>.

²⁸ Lomsadze, Giorgi. 2022. "Scam Call Centers Proliferate in Georgia." *Eurasianet*, June. <https://eurasianet.org/scam-call-centers-proliferate-in-georgia>.

²⁹ Bruce Zagaris, "Transnational Fraud and Economic Integration," *International Enforcement Law Reporter* 39, no. 4 (April 2023): 169-170

Investigation Orders, and Mutual Legal Assistance requests in connection with these internet fraud cases³⁰. Though the investigations, as pointed out above, have led to multiple arrests, the issue of scammer call centers is not eliminated. In the 2021 SOCTA review for organized crime, a metaphor inspired by the Greek Mythology monster Hydra was employed. The Hydra, a colossal water-snake-like creature with nine heads, became a symbol of the persistent nature of the challenge. It was said that when one tried to sever a head, two more would sprout from the wound, signifying the resilience of organized crime activities despite efforts to eliminate them³¹. Expanding on this metaphor, a more efficient approach to combat organized fraudulent crime networks is to target the very body that holds the faces together, which, in the case of crime networks in Georgia, pertains to the corrupt higher officials benefiting from scammer call centers. Simply arresting the lower-level employees of these companies would only result in the emergence of multiple new faces of the monster, perpetuating the cycle of criminal activities.

Conclusion

Overall, the issue of transnational fraud and scammer call centers poses a significant human security threat, affecting individuals and communities worldwide. Despite efforts by law enforcement and international organizations like Eurojust and Europol to combat these criminal networks, their sophistication and ability to operate across borders continue to challenge effective eradication. The situation in Georgia, where scammer call centers have proliferated, underscores the complexity of the problem and the political dynamics surrounding it. The blame game between the government and opposition diverts attention from the core issue, which involves the involvement of corrupt higher officials in supporting and profiting from these illegal activities. To address this human security threat, a more comprehensive and collaborative approach is needed, targeting

³⁰Bruce Zagaris, "Transnational Fraud and Economic Integration," *International Enforcement Law Reporter* 39, no. 4 (April 2023): 169-170

³¹ "Serious and Organised Crime in the EU: A Corrupting Influence," Europol, n.d., p.14, <https://www.europol.europa.eu/media-press/newsroom/news/serious-and-organised-crime-in-eu-corrupting-influence>.

not only the lower-level perpetrators but also the corrupt entities facilitating these criminal operations. Only through coordinated efforts and international cooperation can we hope to combat the growing menace of transnational fraud and protect vulnerable individuals from falling victim to these sophisticated criminal networks.

References:

Bruce Zagaris, "Transnational Fraud and Economic Integration," *International Enforcement Law Reporter* 39, no. 4 (April 2023): 169-170.

Cameron, Sarah, and Sarah Cameron. 2023. "Fraud to Be Reclassified as a UK National Security Threat." *ComplyAdvantage*, February. <https://complyadvantage.com/insights/fraud-to-be-reclassified-as-a-uk-national-security-threat>.

Civil.Ge. 2022. "Five Arrested in Alleged International Fraud Scheme." *Civil Georgia*, February 18, 2022. <https://civil.ge/archives/473660>.

Cohen, Carole. 2006. "Consumer Fraud and the Elderly." *Journal of Gerontological Social Work* 46 (3-4): 137-44. https://doi.org/10.1300/j083v46n03_08.

"Finance Minister: 46 Call Centres Operating in Georgia under Investigation for Alleged Illegal Activities." n.d. *Agenda.Ge*. <https://agenda.ge/en/news/2022/1222>.

Gunter, By Max Hudson Simona Weinglass, Mark Turner and Joel. 2023. "On the Hunt for the Businessmen behind a Billion-Dollar Scam." *BBC News*, April 11, 2023. <https://www.bbc.com/news/world-65038949>.

Lomsadze, Giorgi. 2022. "Scam Call Centers Proliferate in Georgia." *Eurasianet*, June. <https://eurasianet.org/scam-call-centers-proliferate-in-georgia>.

Norris, Gareth, Alexandra Brookes, and David Dowell. 2019. "The Psychology of Internet Fraud Victimization: A Systematic Review." *Journal of Police and Criminal Psychology* 34 (3): 231-45. <https://doi.org/10.1007/s11896-019-09334-5>.

Rusch, Jonathan J. 2003. "The 'Social Engineering' of Internet Fraud." United States Justice Department, January. <http://taupe.free.fr/book/psycho/social%20engineering/TheSocial%20Engineering%20of%20Internet%20Fraud.pdf>.