National Crime Agency

Operation Destabilise

Press pack

Content embargoed to 15:30 on 4 December 2024

Images and video can be downloaded on the following link:
https://spaces.hightail.com/space/XgJvpsSBwR

National Crime Agency

Contents

Overview 3
Outcomes 3
Operational impact 4
Laundering methodology 5
Sanctions evasion and supporting the Russian financial sector 6
Supporting ransomware criminals 7
Directing UK-based money laundering 8
Case summaries 8

STRICTLY EMBARGOED TO 15:30 ON 4 DECEMBER 2024

Overview

- Operation Destabilise is the NCA-led investigation into multi-million dollar Russian money laundering networks, who provide services to a range of criminal actors.
- Investigators have identified two Russian-speaking networks collaborating at the heart of the criminal enterprise; Smart and TGR.
- Smart and TGR's reach spans 30 countries, from the UK and mainland Europe, to the Middle East, Russia and South America.
- They work on behalf of Russian oligarchs and elites, sanctioned individuals and entities, ransomware groups, and organised crime groups in the UK and around the world.
- This includes the Kinahans, the notorious family-run crime syndicate, responsible for trafficking drugs and firearms into the UK and around the world, who were sanctioned by the US in 2022.
- From late 2022 to summer 2023, the Smart network was also used to fund Russian espionage operations.
- Though distinct, Smart and TGR are connected through assisting each other in money laundering activities. Their complex scheme involves them collecting funds in one country and making the equivalent value available in another, often by swapping cryptocurrency for cash.
- This provides a mutually beneficial service from which the networks profit. The service streamlines the movement of cash generated by crime groups in the West, while simultaneously laundering crypto for cyber criminals, and helping Russian oligarchs and elites to bypass sanctions.
- Op Destabilise has been delivered alongside international partners including the Department of the Treasury's Office of Foreign Assets Control (OFAC), the Federal Bureau of Investigation (FBI), the Drug Enforcement Administration (DEA), An Garda Siochana in Ireland, and the Direction Centrale de la Police Judiciaire, as well as a number of UK law enforcement partners.
- The NCA also worked closely with authorities in the UAE to disrupt related money laundering activities.

Left: Ekatarina Zhdanova (Smart) Right: Elena Chirkinyan and George Rossi (TGR)

STRICTLY EMBARGOED TO 15:30 ON 4 DECEMBER 2024

Outcomes

- Operation Destabilise has exposed billion-dollar money laundering networks operating in a way previously unknown to international law enforcement or regulators.
- For the first time, we have been able to map out a link between Russian oligarchs and elites, crypto-rich cyber criminals, and drugs gangs on the streets of the UK. The thread that tied them together – the combined force of Smart and TGR – was invisible until now.
- Their criminal scheme has been disrupted at every level. NCA-coordinated activity has so far led to 84 arrests, with many already serving prison sentences, as well as the seizure of over £20m in cash and cryptocurrency.
- As well as taking out the UK cash couriers taking direction from the laundering networks, the NCA and its international partners have delivered significant disruptions against the leaders who have masterminded this new generation laundromat.
- The head of the Smart network has been identified as Ekaterina Zhdanova, a Russian national. Zhdanova worked closely with Khadzi-Murat Dalgatovich Magomedov and Nikita Vladimirovich Krasnov to facilitate her money laundering activities.
- The head of the TGR Group is George Rossi. Rossi's illicit operation is underpinned by Elena Chirkinyan, his second in command, and Andrejs Bradens (AKA Andrejs Carenoks), a senior figure in the network.
- Zhdanova was sanctioned by US OFAC in November 2023.
- Magomedov, Krasnov, the leading figures of TGR and four associated businesses, including TGR Partners, TGR DWC LLC, TGR Corporate Concierge Ltd, and Siam Expert Trading Company Ltd, have been also been sanctioned by US OFAC today [04/12/2024], with designations linking them to Zhdanova.
- The sanctions detail how the heads of these global laundering networks were involved in bypassing UK, US and other western sanctions, UK cash-based money laundering, laundering through the UK property sector, enabling Russian oligarchs and elites to move funds to the West, as well as laundering for ransomware and other crime groups.
- A seventh individual, who was a global money laundering facilitator with strong links to one of the networks, has also been arrested by the NCA's international partners. This individual was the leading figure of an international controller network, trusted by criminals to receive money in one part of the globe and make it available elsewhere.

Operational impact

- This operation harnessed the capabilities of experienced investigators and intelligence professionals as well as experts in data, cyber and finance – both traditional and virtual. The cumulative effect of layering these capabilities has enabled the NCA to identify the threat posed by the TGR and Smart groups and degrade it. Without this unified approach, it is possible that the networks would continue to offend undetected.

- Through arrests and cash seizures, the NCA and UK law enforcement partners have reduced community harm across the UK and prevented the reinvestment of funds back into criminal enterprises.
- This operational activity in the UK did not go unnoticed by the criminal networks investigated. In late 2022 and early 2023 members of the networks were believed to have reservations over operating in London, likely due to potential law enforcement activity.
- In late summer 2024, Russian-speaking laundering networks operating in London were charging high-commission rates and believed that it was difficult to work in the city.
- This activity has also been extremely costly to the networks, who are assessed to operate on very low profit margins - often charging as little as 3% commission for the amount laundered. Based on this figure, they would need to launder around £700m for free to pay back the £20m seized by the NCA and partners.
- Based on an average 'street level' purchase of 3.5 grams of cocaine and the average UK purchase price throughout 2023, this figure would represent over 70,000 street level purchases of cocaine. This indicates how Op Destabilise has disrupted criminal activity in the UK, targeting individuals working at all levels of money laundering networks to protect UK communities from harm.
- The sanctions imposed against the primary subjects of Op Destabilise will restrict their access to the legitimate global financial system, particularly the US system, a core element of the service they provided.
- Financial organisations across the world, dealing in both fiat and crypto currencies, are now aware of the threat posed by TGR and Smart, enabling them to impose measures to prevent their organisations being used to enable the laundering of criminal funds.
- Together with the arrests, the sanctions have shown that members of TGR, Smart, and those associated with them are of interest to international law enforcement and will be pursued accordingly.

Laundering methodology

- The networks investigated are responsible for laundering billions of US dollars annually
- Smart and TGR operate internationally and, while they use a range of methods to facilitate large cross-border transactions, they are heavily enabled by the use of cryptocurrency.
- The networks have multiple links into the Russian financial sector and often routed funds through the Middle East.
- They service they provide involves collecting funds in one jurisdiction and making the equivalent value available in another, often by swapping cryptocurrency for cash.
- For example: A Russian cybercrime group has $1 million in cryptocurrency, paid by a victim following a ransomware attack. And in the UK, a drugs gang has made the same amount in cash, which now needs to be laundered.
- The networks would arrange for the UK drugs gang to be paid in crypto in exchange for their cash. The cash would then be laundered out of the country through cash rich businesses, such as construction companies, and further laundered through a series of international business accounts.

- After the exchange, the drugs gangs use the crypto to buy more drugs or firearms, causing harm to communities across the UK, without the need to move any physical money across borders. And the equivalent value of the cash would make its way back to the Russian cyber criminals.
- Investigators have seen similar exchanges, where cash handovers were followed almost immediately by the movement of crypto of the same value, taking place on a large-scale across the UK. And this is likely replicated in a number of other countries in the West.
- But this is just one method the networks use to move billions around the world. They also help wealthy Russians to bypass laws and regulations that would prevent them from investing in the UK. They use a complex laundering process to mask the source of the funds, enabling their clients to secretly buy property and high-end goods in the UK.
- These money laundering networks enable serious criminality in the UK and threaten the integrity of our economy. Their service fuels the drugs trade and the associated violence committed by gangs, and deprives society of legitimate funds that pay for schools, hospitals and social services.

Sanctions evasion and supporting the Russian financial sector

Providing a gateway to Western economies:

- Following Russia's invasion of Ukraine in February 2022, the UK, US and the European Union imposed expansive sanctions on the Russian financial system.
- The services provided by the TGR Group and Smart enable Russian oligarchs and elites to access Western financial markets that may otherwise be denied to them through sanctions and other financial regulations. This type of activity provides a release valve on the pressure that would have otherwise been applied by UK and partner nation sanctions to the Russian financial sector.
- In March 2022, Zhdanova and members of the TGR Group used cryptocurrency and the UK financial sector to move over £2m into the UK to purchase properties for a Russian client. The networks attempted to mask the source of the funds through a complex laundering process and bypass know your customer checks.
- Assets illegally moved to the UK will be identified and pursued by the NCA and its partners in the public and private sectors.

Garantex:

- TGR and smart make heavy use of cryptocurrency to enable their global laundering operations. The cryptocurrency addresses of both networks display heavy exposure to Garantex, a Russian crypto-currency exchange sanctioned by US OFAC on 05/04/2022 and the UK FCDO on 04/05/2022.
- The majority of Garantex's operations are carried out in Moscow, including at Federation Tower, and in St Petersburg. Federation Tower is reportedly fortified against 'missiles and explosions' and has been home to over a dozen companies that convert crypto-currency to cash.
- According to open source reporting, at least four companies operating from Federation Tower have been linked to money laundering activities related to ransomware.

- Prior to designation, over $100 million of Garantex transactions were linked to criminal actors, including $6 million from Conti, a ransomware-as-a-service group with assessed links to the Russian Intelligence Services, and $2.6 million from the Hydra darknet marketplace.
- Open source reporting indicates that Garantex has been linked to payments to companies for components of weapons used by Russia in its invasion of Ukraine. The same reporting indicates that the founder of Garantex has advertised the use of cryptocurrency to bypass sanctions.
- It is suspected that Garantex has either benefitted from or supported the government of Russia by carrying on business in the financial services sector. Smart and TGR have extensively transacted with Garantex after the dates that it was sanctioned, layering and integrating funds into the global financial system. As such it is suspected that, after Russia's illegal invasion of Ukraine, TGR and Smart have supported the Russian financial sector by laundering funds linked to Garantex and integrating them into the global financial sector.

Russia Today:

- In 2023, Elena Chirkinyan of the TGR Group, was involved in transferring funds out of Russia, most likely to support the activities of a Russian-language media organisation in the United Kingdom. These funds are alleged to have originated from Russia Today. On 31/03/2022, the UK sanctioned TV-Novosti, the Kremlin-funded entity who own Russia Today (RT).
- In September 2018, two Russian military intelligence officers were charged in absentia in relation to the attempted murder of Sergei and Yulia Skripal and the use of the Novichok nerve agent. The two officers later appeared on RT claiming to have been tourists. RT was fined by OFCOM due a serious breach in its impartiality rules in relation to the Skripal and other coverage.
- On 18/03/2022, OFCOM revoked RT's licence to broadcast in the UK. More recently, RT have been linked to a malign influence campaign in the US.

The Russian technology sector:

- Siam Expert Trading Company Ltd., a Thailand-based company associated with Bradens that was sanctioned by OFAC today [04/12/2024], facilitated the export of electronic components to Russia.

Supporting ransomware groups

- The services provided by these networks allow ransomware actors to benefit from their crimes and proliferate.
- Zhdanova provided services to members of the Russian Ryuk ransomware group. In 2021, Zhdanova laundered over $2.3 million of suspected victim payments on behalf of a cyber criminal who deployed a Ryuk attack. Ryuk has been used to target thousands of victims worldwide.
- On 09/02/2023, the NCA announced investigations, alongside FCDO and US OFAC sanctions against the crime group involved in the Trickbot, Conti and Ryuk ransomware strains. The crime group was the subject of further sanctions in September 2023.

- The NCA assesses that the group was responsible for extorting at least £27m from 149 UK victims including hospitals, schools, businesses and local authorities. However, their true impact is likely to be much higher.
- The deployment of ransomware remains the greatest cybercrime threat, the largest cyber security threat, and is a threat to UK's national security.
- Ransomware attacks can have a significant impact on victims due to financial, data and service losses which can lead to inaccessible public services and other significant risks.

Directing UK-based money laundering

- Smart and TGR play a significant role in cash-based money laundering in the UK. Many of the money laundering transactions were brokered by Zhdanova and Magomedov. Krasnov would work with courier networks in the UK to arrange for the cash to be collected from OCGs such as drugs gangs, then arrange for it to be converted.
- TGR and Smart coordinated their activity, with members of the TGR group receiving large volumes of cash on behalf of Zhdanova and facilitating the conversion, making the equivalent value available in cryptocurrency.
- The NCA and policing partners evidenced this exchange taking place at scale across the UK, where street-level cash handovers were followed almost immediately by a movement of cryptocurrency of the same value.
- One courier network investigated conducted cash handovers in 55 different locations across England, Scotland and Wales and the Channel Islands, over a four-month period. They did so on behalf of at least 22 suspected criminal groups operating in the UK, supporting them to fund further criminal activity.

Case summaries

Case Summary 1:

Between July 2022 and September 2023, Semen Kuksov and Andrii Dzektsa managed cash couriers in the UK to collect criminal money and deliver the laundered money overseas. During a 74-day period, they helped to launder £12,329,460.

Left: Kuksov Right: Dzektsa

Kuksov, the son of a Russian oil executive, coordinated with Nikita Krasnov. His network is known to have laundered further funds across Europe and beyond and he also admitted to operating an underground cryptocurrency exchange.

Following an NCA investigation, Kuksov and Dzektsa were sentenced to five years seven months and five years imprisonment respectively on 01/02/2024. Over £1.3 million was seized from Kuksov's network by investigators as well as over $500,000 of cryptocurrency.

The NCA and international partners arrested a series of couriers linked to Kuksov and his associates. One courier linked to Kuksov's network, Igor Logvinov, was arrested by An Garda Siochana in Ireland and sentenced to 3 years imprisonment.

Kuksov directed and exercised influence over others involved in money laundering. He did this over a significant period of time and across borders, demonstrating a high degree of planning. Though subordinate to Kuksov, Dzeksta managed couriers, giving them directions as to when and where to collect and deliver cash.

Kuksov's network used physical tokens for cash handovers, a common practice for cash-based money launderers. Tokens are usually low denomination bank notes which bear a unique serial number. This serial number is passed on before a cash handover takes place and when the two parties meet, the person collecting the cash will produce the bank note to prove that they are the intended party. The token is usually then handed over, acting as a receipt that the handover has taken place.

Saju Sasikumar, NCA Operations Manager, said: "Semen Kuksov ran what was, in effect, a professional banking service for criminals around the world, who could not access the legitimate banking system due to the source of their funds. He arranged collection of cash from groups that wanted rid of it and delivered cash to groups that needed it.

"Money laundering is often seen as a victimless crime, but without the services of people like Kuksov and Dzektsa, the business model of criminal groups they are enabling will be broken as they will not be able to access their ill-gotten gains.

"It is for this reason the NCA will continue to pursue professional money launderers to degrade the business model of the laundering networks and thus protecting our communities from the inherent risks posed by the criminal groups they are laundering for.

"This painstaking investigation was only possible due to the dedicated and tenacious detective work conducted by our Investigators, together with joint working with international law enforcement partners and partners in CPS."

Case Summary 2:

On 29 November 2021, Fawad Saiedi was stopped by the Metropolitan Police Service (MPS) whilst driving a vehicle. A search of the vehicle found in excess of £250,000 in cash. A search of Saedi's home found a further £24,500 and a cash counting machine. He was being directed by Nikita Krasnov and Eketarina Zhdanova.

Saiedi was a courier and a collector (directing other couriers to collect cash).

On 03 May 2022, following an investigation by the NCA and MPS Organised Crime Partnership, Saiedi pleaded guilty to possessing and transferring criminal property. The Crown assessed that the value of criminal property transferred was £15,667,720. This was uncontested. Saiedi was sentenced to 4 years and 4 months imprisonment.

Case Summary 3:

In October 2021 a States of Jersey Police investigation focused on money laundering activities of Eshonkulov, Umurzokov, and Bataa who were attempting to launder approximately £60,000 in used Jersey bank notes in Jersey.

Evidence from seized mobile phones, documentation, receipts and lists revealed their involvement in sub-letting UK properties paid for in cash from drug trafficking or prostitution.

The seized mobile phones held identities of Uzbekistanis, Hungarians, Latvians and Romanians, believed to have illegally entered the UK, to be housed in properties subject to illegal sub-letting.

Photographs from the seized mobile phones showed:

- Umurzokov counting bank notes and messages indicating travel throughout the UK collecting bags of cash.
- English and Scottish banknotes evidencing the reach of the money laundering network
- Wrapped cash in significant amounts, typically associated to large scale drug trafficking
- Cash laundering using high denomination £50 notes

STRICTLY EMBARGOED TO 15:30 ON 4 DECEMBER 2024

All defendants had large sums of money moving in and out of their UK bank accounts. Substantial amounts of money were transferred to and from UK business bank accounts, mainly through 'ISM Scaffolding Limited', which had £4.31 million passing through its account within 10 months in 2021/2022.

They were charged with offences under Article 31(1) (d) Proceeds of Crime (Jersey) Law 1999 and pleaded guilty to a total of 22 charges of Money Laundering, admitting to work for a UK based organised crime group. They were sentenced by the Royal Court of Jersey for a combined total of 10 years imprisonment.

Within the conclusions, the Jersey Attorney General stated:

"This was a well-planned money laundering operation. An aggravating feature of these offences is that the Jersey bank notes were bought to the island for the express purpose of being laundered here."

Case Summary 4:

On 20/05/2024 an Ukrainian registered Mercedes Sprinter, was intercepted outbound the Channel tunnel. The van had two occupants, both Ukrainian nationals; Taras Hirnyak and Andrii Trachuk. Hirnyak claimed to be taking items to Ukraine for the war effort. A search identified several boxes labelled Asda washing powder found to contain an estimated £1 million in cash.

Hirnyak and Trachuk were arrested and investigated by the NCA and later pleaded guilty at Canterbury Crown Court. They were each sentenced to two years in prison.

Hirnyak and Trachuk are believed to have made multiple previous trips in 2024.

STRICTLY EMBARGOED TO 15:30 ON 4 DECEMBER 2024

Case Summary 5:

On 26/03/2023 Border Force Officers intercepted a Ukrainian registered Mercedes van driven by Ruslan Kaziuk at the Outbound Tourist Controls, Eastern Docks, Dover, Kent.

During a search of the vehicle, Border Force Officers found silver taped packages containing cash in:

- three cardboard boxes containing wax pellets;
- two Bags for Life containing wax pellets;
- concealed inside a white van door, inside the natural space behind screwed down chipboard.

The total cash detected was £2,123,285.00.

The case was referred to HM Revenue and Customs (HMRC) for investigation which resulted in Kaziuk being charged with Money Laundering contrary to Proceeds of Crime Act 2002 s327 (1) and 334. In September 2023 Kaziuk pleaded guilty for the offence on the first day of trial and received a sentence of 5 years and 8 months imprisonment.

Case Summary 6:

On 23/03/2023 NCA officers arrested Andrejs Jasins on suspicion of money laundering at Frankley Services, M5 Southbound, Birmingham and searched his Ford Transit vehicle. Jasins advised that there was a quantity of cash contained within a storage area beneath the front passenger seat.

Three bags were found within the storage area beneath the front passenger seat. Within each bag was a further inner bag within which Officers identified sterling notes estimated to be in the sum of £400,000. The notes were secured with coloured elastic bands. Jasins was charged with money laundering.

Jasins is a Latvian national who flew into the UK the day before his arrest.

In August 2023 Jasins appeared at Worcester Crown Court, and pleaded guilty to the charge. He was sentenced to 24 months and 14 days.

The total cash seized and subsequently forfeited was £357,730.95. The contents of Jasins' mobile revealed a number of photographs indicating a greater level of involvement than that of simply a courier.