Financial Crimes Investigative Summary
Compliance-Sloutions.pro Complex Litigation Support
Cyber Warfare Center Pacific (CYWAR-CENPAC)
Liberty Station USNTC Point Loma CA USA

A British national made his first payment to financial advisor “Liliana” to an account at a Bulgarian company at the neobank Revolut. His case was typical of those examined by Compliance-Solutions.pro as part of a financial crimes investigation. Revolut Group Holding, Ltd. dba Revolut, is a British multinational neobank and fintech company that offers banking services for individuals and businesses. It was founded in July 2015 by Russian businessman Nikolay Storonsky and Ukrainian software engineer Vlad Yatsenko. The company offers services in 48+ countries, though the extent of its banking licenses varies by region. In the UK, Revolut has an "authorization with restrictions" banking license which means it can't accept cash or check deposits, all transactions are virtual and there are no branch offices or customer support call center and a very lax anti-money laundering (AML) and know-your-customer (KYC) policy. Revolut leverages sub-account VIBANS (Virtual International Bank Account Numbers) instead of IBANS (International Bank Account Numbers). IBANS accounts are opened by business customers as a main account holders which then open sub-accounts using a VIBANS account that is managed by the master business account that allows Revolut to obscure the beneficial ownership of wired funds through a sub-account framework that redirects cryptocurrency and bank wires to offshore scammer accounts in Cyprus, Dubai and Bulgaria.

What happens is that Revolut is exploiting loopholes in international banking regulations and gaps in regulatory oversight of third-party money transfer services and financial services consultants that hold themselves out to be an investment brokerages that do not handle cash or check deposits and as such they're not required to follow anti-money laundering laws or the Bank Secrecy Act. So a scammer opens a master business account at Revolut, then the scammer finds a victim to con into making investments in cryptocurrencies, stocks and/or bonds, the victim is given a promotion code and instructed to open a personal account at Revolut using the promotion code which tells Revolut that the account is a sub-account to the scammers master account. The victim opens the account and funds it using their actual bank account, in this case the Royal Bank of Scotland. When the bank wire arrives at Revolut it is deposited into the master account with the scammer responsible for "loading" the victims account with the funds received, which never happens.

In some cases, victims would be walked through the process of converting funds to crypto, then they would send it on to wallets held by the scammers. In others, victims would be talked through setting up accounts with online-only “neobanks” such as Wise, Revolut and Wirex, and sometimes supplied with scripts for answering questions about

their outward transactions — in the event anyone asked. Liliana the scam advisor, who the British national communicated with over WhatsApp, urged him to open an account with UK digital-first bank Chase. She provided him with precise instructions for what he should do if Chase questioned transactions: tell the bank that the 7,000 pounds were for “theater tickets”.

By examining financial documents from a deep-web leaked data trove, Compliance-Solutions.pro has uncovered how a vast network of middleman payment service providers — which included cryptocurrency exchanges, wire transfer companies — enabled the movement of victims’ payments. These "payment service providers" were not licensed and in most cases did not appear to correspond to real legal entities. They allowed scammers to access international payments, while distancing themselves from the transactions.

One payment service provider, operating under the name Bankio, provided scammers with instant access to bank accounts they could instruct their victims to send money to. Bankio, and other providers like it, would create invoices for non-existent goods or services that scammers could use to justify the transfer of funds.

Despite the slick branding, there is no corporate entity registered under the name Bankio, and investigators could not determine who was behind it. Evidence from the leak strongly suggests it is connected to a similar service provider, Anywires, which was widely used by the Israeli/European operation. In internal documents, Bankio and Anywires were referred to interchangeably. The movement of funds in these operations was complex by design. To wit: “In one money-moving scheme traced by investigators, victims’ funds were sent to a group of firms registered in Spain and the United Kingdom, who moved it among themselves before routing it to a second tier of firms, mostly in the UK, the United Arab Emirates, and Hungary. The money then flowed to other firms, disguised as consultancies, in Cyprus and North Macedonia, before the trail was lost.”

Another enabling factor was Virtual International Bank Account Numbers, or VIBANs. Traditional banks are associated with IBANs, which are connected to one specific bank account at that institution. A VIBAN, however, allows certain bank clients — typically other financial institutions or payment processors — to set up sub-accounts connected to a single master account. Compliance-Solutions.pro facilitated the British nationals investigation and was ultimately able to get some of the $380,000.00 pounds stolen savings back through the Compliance-Solutions private fund recovery and asset tracking protocol, the ordeal placed the British national under enormous stress and left him feeling humiliated. Untold thousands around the world have faced similar personal devastation and financial ruin. That’s why we’ll keep trying to shed light on how scammers are exploiting weaknesses and loopholes in the global banking system to

siphon victims' money away. In order to do that we need to start at the beginning of the trail, and that is with Revolut. To begin with, Resvolut was founded by Nick Storonsky, a Russian national with British dual nationality that is an honors graduate from the Moscow Institute of Physics and Technology. For anyone who does not know, the Russian Federation does not offer scholarships to their elite universities and institutes by picking names out of a hat. Usually the selection process involves a future state need for a specific element that is crucial to an operation that is being contemplated, and the selection process naturally includes the involvement and recommendations of any number of Russian intelligence services whose job it is to vet potential candidates. So when Storonsky accepted the scholarship, he also accepted the fact that his entire career would be scrutinized by the Russian intelligence community, and most probably he was a willing participant in the operation and even more probable that he was actually recruited as a Russian intelligence officer. The Moscow Institute of Physics and Technology closely cooperates with the Military and Industrial Complex of the Russian Federation. It was the Moscow Institute of Physics and Technology which developed drone systems used by the Russian military and for a contract awarded by the Russian Ministry of Defence. Besides, the institute includes a laboratory which supports the Russian military and space sector. The Moscow Institute of Physics and Technology is one of the Russian institutions which train professionals for the Russian defense and industrial complex and intelligence community, collaborating with the Russian defense research organization within different research projects. It is already under the sanctions of Ukraine, EU, Great Britain, USA, Canada, Switzerland, Japan, New Zealand. The institute fund is sponsored by numerous sanctioned Russian arms and weapons manufacturers, including:

Tactical Missiles Corporation JSC
Uralvagonzavod (tanks producer)
Mashynostroyenia Scientific and Production Association JSC (develops Russian missiles)
United Aircraft Corporation (produces Russian combat aircraft)
Concern Sozvezdie JSC (develops Radioelectronic warfare systems for the Russian Army)
Almaz-Antey open JSC (produces Russian air-defence complexes)
Moscow Institute of Thermal Technology Corporation JSC (produces Russian missiles)

It is a matter of fact that Storonsky is a Russian physics scientist and a Russian intelligence asset, as that is the only path to membership in the Russian Academy of Sciences. It is also a matter of fact that between 20012 and 2014 the Russians were developing an alternative to the Western controlled SWIFT international financial settlement system due to their concerns that Western sanctions would prohibit Russian companies and nationals from using SWIFT, without an alternative the Russian economy would be severely impacted by sanctions which became more urgent the

moment Russia invaded Crimea. Storonsky's mission was to develop the alternative financial framework that would allow Russians to bypass sanctions and have unrestricted access to global financial markets. Revolut is that alternative framework. Largely unregulated and at risk, Storonsky would not have had developed the Revolut platforms source code without including a backdoor, which Russian intelligence has the key to. That means that the Russians can misappropriate, seize, freeze or just outright steal the deposits of over 50 million Revolut personal customers and 500,000 business customers in 160+ countries totaling loses in excess of 18.2 billion dollars, at will, whenever they feel it's time. Right now, Revolut has Hungarian and Montenegro business accounts that have thousands of sub-accounts of Russian nationals that use the Revolut account as if they are Hungarian or Montynegran nationals and not Russian nationals thereby avoiding sanctions and allowing them to enjoy trade and commerce globally, as if there are no sanctions.

It's a well established standard operating procedure among global intelligence agencies to install backdoors in the source code for any software platforms that they develop as it's the only way to control the software and it's users, without leaving any tracks to follow. A perfect example is found with the founder of Telegram messenger platform, Russian national Pavel Durov, a computer scientist from St. Petersburg University developed the Telegram source code with the hidden back door. Because Durov was managed by a GRU (Russian military intelligence), they had the keys to the backdoor which allowed the GRU to monitor Telegram channels that Russian soldiers and officers used to communicate, many time the communications involved spreading classified material, unit scuttlebut and tactical methods that should not be in the channel to begin with. The Russian Ministry of Defense (MoD) encouraged the use of Telegram by Russian soldiers because it was how the MoD kept informed about what was going on at the unit level with rank and file troops as well as the officers constant use of Telegram channels to relay tactical updates for troop movements and artillery counter-battery response.

When Durov decided to abandon ship and voluntarily surrender to French witness protection officials, which was spun as Durov arrested on a host of charges related to Telegram use, it was all a cover story to temporarily mislead Russian officials without letting on that the Western intelligence agencies were given the key to the backdoor by Durov in exchange for protection from Putin's assassins. All of that military traffic on all of those Telegram channels is then in Western hands, which represented a very serious blow to the Russians and an absolute goldmine for the West. I'm not a gambling man, but I will wager that within the near future, we're going to see Storonsky abandon ship also, the cover story will be he's arrested for money laundering and he'll be taken into protective custody and hand over the key to the backdoor to Revolut because the West can't afford not to shut Revolut down, they need the transaction data to identify the prolific money launderers, black market suppliers, sanction evaders, politically exposed

persons, ultra high-net worth individuals, beneficial owners and scammers that cost the global community 3.4 trillion dollars annually.

Let's get back to Revolut, as stated previously, the neobank has 50 million + personal accounts, 500,000+ business accounts, deposits in excess of 18.2 billion dollars distributed throughout 160+ nations in 36 different currencies, they have virtual checking/savings/investment accounts, a crypto exchange called Revolut RAMP Crypto and Revolut X Crypto and an investment brokerage specializing in stocks and bonds. The business is 100% virtual with no brick and mortar branches, no customer support call centers, and no cash or check deposits. Technically they are considered a 3rd party money transfer provider, but because it does not accept cash or checks, it's not considered a bank, even though they were licensed by the Bank of Lithuania in 2018 and a British restricted banking permit in 2020, they claim to have actual banking licenses in 30 countries and they have other licenses and permits that gives the impression of legitimacy as a financial institution.

The Board of Directors: The Chairman is Martin Gilbert, a British national with Aberdeen Asset Management and Deloitte that specializes in financial audits and accounting, Director Storonsky worked at Credit Suisse and Lehman Brothers, Vlad Yatsenko, a Russian national from UBS Financial and Deutsche Bank, Director Michael Sherwood with Goldman Sachs Group, Director Carolyn Britton with Deloitte and the Make-a-Wish Foundation, Director Ian Wilson with Santander UK and Virgin Money, Director John Sievwright with Merrill Lynch Global and Bank of Tokyo, and Director Dan Teodosiu with Google and Microsoft. That's who's running the day to day operations of Revolut, they're the ones that shared the loopholes and regulatory gaps in oversight that they have exploited to facilitate the Russian evasion of sanctions, we just happened to stumble across it while investigating scammers that are using the same methods, except to steal money, not to evade sanctions. The Board of Directors reflects the expertise required to become a viable alternative to SWIFT using all of the exploitable vulnerabilities in the current Western dominated financial transaction processing pipelines, that requires special insider knowledge, the type of knowledge that senior -level management at Goldman Sachs, Credit Suisse, Lehman Brothers, Merrill Lynch Global, Bank of Tokyo, Santander and Deloitte have accumulated after years of direct supervision of the SWIFT framework.

So, Resolut is 100% virtual, it exists in cyber space, it has no physical location where it exists but is everywhere, the closest that it comes to a tangible item is through the registration of their virtual domain, in this case the NameCheap domain name registrars were used to create the revolut.com domain which is using a bullet-proof host in the country of Montenegro and assigned a shared IP Address at 162.159.140.233 using CloudFlarenet-US AS 13335 outbound encrypted tunnels to hide financial transactions and facilitate untraceable cryptocurrency and fiat currency exchange transactions.

revolut.com has 8 sub-domains; app.revolut.com (log in), get.revolut.com (signup), help.revolut.com (investor faq), help.revolut.combanking faq), help.revolut.com (customer faq), developer.revolut.com (API) and cdn.revolut.com (consumer security insight report) they all share the same IP address, using the same host and autonomous network built on CloudFlare outbound encrypted tunnels, which CloudFlare provides free of charge to any cyber crook that wants to use it. All the Russian hackers and Eastern European scammers are using the CloudFlare encrypted tunnel protocol to hide their activity, Revolut is no different. All of their advertising is done through social media platforms where their username is @revolutapp on Facebook, Instagram, Twitter (X), LinkedIn and Tik Tok where they have millions of followers. The $18.2 billion in deposits are virtual, not physical. So there's no vault with $18.2 billion dollars in hard currency and precious metals, it's all just entries in a ledger that can be manipulated at will, it's unregulated, not subject to independent audit by regulatory authorities, and there's no proof that any of it exists outside of a few elementary references that have no place of business listed and an accounting department that keeps no hard copies, of anything. This is a long summary because it takes time and space to articulate a 100-hour financial crime investigation into a 30 minute disclosure.

Revolt Holding Group Limited, is a British company # 12743269 filed July 15, 2020, their annual report can be found here:

https://find-and-update.company-information.service.gov.uk/company/12743269 under "File History" scroll down to 192 page Annual Report

Storonsky is the person with significant control, the nature of the control is the right to appoint and dismiss directors at will, and he's not listed as a Russian national with the Company House Business record repository, he's listed as British and residing in England as the Chief Executive Officer. Getting a British second passport does not make a persons nationality British, anymore than getting a second passport from Switzerland doesn't make a person Swiss. He's still a Russian national, just with a British passport, until he would renounce his citizenship, which hasn't been done. There's a concerted effort by the board to bury the Russian connection and not have Revolut associated with anything Russian, and for very good reason; They don't want any questions about Russia intelligence services involvement with the development of the Revolut platform, because they know, just like I know, that the connections are discoverable if someone knows what they're looking for. We know what we're looking for and we found it.

Revolut offers banking services including GBP and EUR bank accounts, debit cards, credit cards, currency exchange with over 25 fiat currencies, stock trading, cryptocurrency exchange and peer-to-peer payments. Revolut's mobile app supports spending and ATM withdrawals in 120 currencies and transfers in 36 currencies. Similar multi-currency features are available from competing fintech companies. Revolut's

credit card is available in Poland, Lithuania, the United States, and Ireland. Crypto cannot be deposited or spent, only converted back to fiat inside Revolut. Additionally, Revolut banks with Metropolitan Commercial Bank of New York, which does not allow the transfer of fiat money to or from cryptocurrency exchanges. Resolut Securities US Inc is a Delaware corporation whose majority shareholder (75+%) is Revolut Holdings US Inc, another Deleware corporation, with the majority stock ownership (75+%) belonging to Revolut Group Holdings Ltd, the British parent. As of June 2024, Revolut has reached 45 million customers globally. In August, the company was seen to be preparing for a potential IPO on the Nasdaq in the United States with an expected valuation of approximately £45 billion, although UK politicians were said to be pushing for a London listing. The company also doubled its headcount over the past two years, employing over 8,000 people in more than 25 countries. The company faced criticism from local Portuguese banks about unfair competition after its subsidiary, "Revolut Bank UAB", was granted a full banking license by the ECB. Revolut was also granted a British banking license the following month, though with restrictions via the standard "mobilization" stage.

A report in October 2024 found that Revolut was named in more fraud complaints in the UK than any major bank in the country, sparking a debate on the effectiveness of its security controls. It was stated that many customers had to turn to the financial ombudsman service after falling victim to fraud earlier that year. By the end of 2024, Revolut reported having 50 million registered users globally. In 2023, they had over one million daily active users. So does that sound like a system that was designed to be an alternative to SWIFT, bypass sanctions and escape regulatory oversight. Revolut uses a public blockchain ledger that's immutable to record transactions, all of the transactions of the entire financial infrastructure are permanently entered into the ledger.

We use a blockchain transaction inspection tool that can search by deposit address, so it was easy to track the British national victims $380,000.00 pounds that were bank wired from his savings account at the Royal Bank of Scotland to a third party payment processing provider going by the assumed name of Bankio (bankio.co.uk 188.114.96.3) hosted on CloudFlare AS 13335 in Amsterdam, same autonomous system as revolut.com, they received the funds through Danske Bank in Warsaw, Poland where it was credited to a VIBAN business account whose beneficial owner is an account information service provider in Bucharest Romania. Danske Bank wired the funds to Alpha Bank's eBanking platforms commercial trade accounts in 8 equal payments to Bankio payment initiation service providers in Austria, France, Netherlands, Poland, Romania, Spain and Switzerland before ultimately ending up in the Grand Bahama Bank and Trust in Nassau, Grand Bahama in a commercial IBAN account in the name of Resolut Holdings Bahama, Ltd.

Based on the volume of approximately 100 billion dollars in transactions a year the Resolut platform has a hard currency and precious metal warchest in the Bahsamas worth an estimated 2.8 billion dollars, the beneficial owner report list's Nikolay Soronsky as the principle owner of Resolut Holdings Bahama Ltd. He's a very wealthy man, and he just received an 80% pay raise. Most of the funds in the warchest can be traced back to other fraud victims in the UK, and there's really no reason not to believe that Resolut is not just one big money laundering operation that also perpetrates frauds on it's own customers. Remember the financial consultant Lilian? The one who scammed the British victim, she was listed as a manager with Revolut Technologies Inc that trades through Revolut Securities Inc and supplies automated investing technology at Revolut Wealth Inc. It's pretty coincidental that she has the same address as the registered agent for the Delaware company Revolut Holdings US Inc.

Recommendations:

Share intelligence with our Federal partners at the U.S. Treasury Departments Financial Crimes Center (FinCEN), the U.S. Securities Exchange Commission and U.S. banking regulators at the Federal Reserve Board, if that is a viable option in our clients opinion, it’s up to the client, not the investigators, to decide what to do with the investigative findings. Absent the express informed consent of the client Compliance-Solutions.pro has no independent authority to act unilaterally on matters of disclosure unless it’s for a very compelling reason. We’re bound by confidentiality and non-disclosure agreements that are backed by a $5 million dollar specific performance bond that guarantees total secrecy.

Notify [classified] at [classified] citing prolific money laundering and sanction evasion and request the IC IG ascertain what relationship, if any, the [classified] had [classified] from [classified] Russian Milblog channels on Western versions of Telegram using [classified] toolset monitoring channel “Intel Z” operated by the GRU and [classified] for launderers to share transaction routing and [classified] [classified] [classified].

Immediate Action Request: [classified]

Report partially redacted for operational security considerations
END OF REPORT