

CYBER
THREAT
ANALYSIS
RUSSIA

Recorded Future®

By Insikt Group®

March 23, 2023

SANCTIONS



Russian Sanctions Evasion Puts Merchants and Banks at Risk

Executive Summary

Cybercriminals devise and execute various workarounds to legalize their illicit income. After international sanctions were leveled against Russia in the wake of Russia's full-scale invasion of Ukraine, ordinary Russian consumers have likely resorted to similar workarounds to obtain goods produced abroad.

Recorded Future has identified prepaid cryptocurrency virtual credit cards and mail forwarding services — also known as “reshippers” — as methods that can potentially be exploited to illegally bypass sanctions. International financial institutions and merchants that are indirect participants of these workarounds may be at risk of falling under secondary sanctions. This risk could be greatly reduced by implementing more stringent verification procedures for the services and transactions involved in these workarounds.

Key Findings

- Many crypto services allow customers to register prepaid cryptocurrency virtual credit cards with minimal or no verification. This lack of verification and dark web sources indicate that these prepaid cryptocurrency VCCs can be used for sanctions evasion.
- Various mail forwarding services allow Russian customers to order goods produced from abroad. Purchases and deliveries can be funded through various means, including cryptocurrency and Russian-issued payment cards. Although these services publish lists of restricted goods that they claim they are unable to ship, dark web sources indicate that they can be used to receive goods that are subject to export controls.
- We registered a prepaid cryptocurrency VCC using one of the crypto services described above. Open source analysis revealed the payment card's bank identification number (BIN) was issued by a US financial institution.
- It is likely that additional financial institutions and merchants are also being enlisted as unwitting participants in sanctions evasion schemes that involve prepaid VCCs and mail forwarding services. If this is the case, they may be at risk of secondary sanctions.

Background

Beginning on February 24, 2022, the US and 37 other countries implemented sweeping sanctions against Russia in response to its unprovoked invasion of Ukraine. These ongoing sanctions are explicitly intended to degrade Russia's ability to wage war in Ukraine, and they include exhaustive restrictions on the export to Russia of luxury goods ranging from garments and accessories to high-end electronics, spirits, and even billiard sticks. [1, 2] According to the US Bureau of Industry and Security (BIS), the proscription of these exports is “intended to steadily increase the financial consequences on Russia ... as a result of Russia's invasion of Ukraine.” Altogether, these measures appear to be having the desired effect. In October 2022, the US Department of State [assessed](#) that “US sanctions and export controls have severed Russia's access to key technologies and industrial inputs that erode its military capability”.

Similarly, the European Council [estimated](#) that Russia's GDP had contracted by anywhere from 2.2% to 3.9% in 2022, undermining Russia's ability to finance its war.

Governments have not acted in isolation, either. Over 1,000 companies motivated by a combination of outrage and fear of secondary sanctions have voluntarily [suspended operations](#) in Russia. Among these are Visa and Mastercard, which at the time of their withdrawal controlled about 70% of the Russian debit card market.

At the same time, technical and legal barriers are unlikely to significantly harm Russian cybercriminals' efforts to monetize their illicit earnings. We previously [predicted](#) that international sanctions and the accompanying decisions of private companies to cease or reduce operations in Russia would likely encourage criminal buyers to reship and resell foreign goods on the Russian market. This is because any shortage of foreign goods on the Russian market that are obtained through legitimate sources likely creates corresponding demand for the same goods obtained through illicit sources. This presents cybercriminals with an opportunity to earn increased returns from their fraud cash-out schemes.

Threat Analysis

Russia Seeks to Evade Sanctions to Support War Effort

As sanctions have intensified against Russia, so have Russia's will and ability to defy them. In mid-2022, Russia [relaxed](#) regulations that banned parallel imports, a move designed to strengthen the Russian economy. In [April](#) and [September 2022](#), the US Department of the Treasury (USDT) designated 64 individuals and entities that were actively involved in attempts to help Russia evade sanctions to fund its war effort. In [June 2022](#), the US Financial Crimes Enforcement Network (FinCEN) and BIS urged US financial institutions to remain vigilant against Russian attempts to bypass sanctions. As recently as September 2022, USDT [conceded](#) that Russia could use cryptocurrency to bypass sanctions, and in December 2022, the Center for Strategic and International Studies (CSIS) [discussed](#) various forms that such sanctions evasion might take.

The use of cryptocurrency to circumvent sanctions or other legal barriers is not unheard of. In [May 2022](#), USDT sanctioned Blender.io, a virtual currency "mixer" used by Lazarus Group to launder stolen funds that were destined for North Korea's illegal nuclear weapons program. In [August 2022](#), USDT also sanctioned TornadoCash, another virtual currency mixer used by Lazarus Group for the same purpose. And as recently as January 18, 2023, US authorities [arrested](#) the cofounder of Bitzlato, a cryptocurrency exchange which FinCEN previously labeled as a "primary money laundering concern" related to Russian criminal finance.

Russian Buyers Adapt

As international sanctions undermine Russia's ability to supply its war effort, they also prevent ordinary Russian consumers from acquiring imported commodities. For Russian buyers, robust export controls, financial sanctions, and the near-total withdrawal of luxury brands and global businesses from the Russian market have complicated the purchase of foreign goods. This difficulty has been worsened by the [diminished](#) ability of alternative Russian payment systems like Mir to compensate by expanding operations abroad.

As a result, Russians have begun resorting to intricate schemes to obtain goods produced abroad. Previously, only criminal enterprises possessed the resources, knowledge, and connections to implement these schemes, largely for the purposes of laundering their ill-gotten profits. Russian individuals and companies now rely on similar workarounds to organize parallel imports — that is, imports outside of formal distribution channels — which may be used to obtain restricted goods. [Parallel imports](#) are often organized using third-party shipping schemes facilitated by intermediaries in “friendly” neighboring countries, particularly member-states of the Eurasian Economic Union (EAEU, or EEU) like Kazakhstan and Armenia.

While it is improbable that all of these “gray imports” are illegal, it is highly likely that at least some of these workarounds are used for illegal ends, including sanctions evasion. In a particularly telling example, stories [emerged](#) in May 2022 that computer chips from US dishwashers were being used to produce or repair Russian military equipment. Likewise, trade statistics [reveal](#) that the import of breast pumps to Armenia and Kazakhstan spiked sharply in the first half of 2022 despite national birth rates for those periods dropping, suggesting that these products were being reshipped to Russia as parallel imports, possibly to obtain electronics crucial for Russia's war effort.

Prepaid Cryptocurrency Cards Help Russians Circumvent Financial Sanctions

Sanctions and the suspension of major card networks' operations in Russia complicate the task of making international purchases with rubles. Historically, one workaround has been to [obtain payment cards from banks in neighboring countries](#), then use these cards to order subscriptions or goods that are later delivered through intermediaries in neighboring countries. In many ways, this is an adaptation of a commonly used scheme among Russian “carders”, who fraudulently purchase goods using their victims' payment cards before organizing delivery to Russia through intermediaries.

For example, the Telegram channel “Tekhnika BestShopx” markets third-party delivery services to Russian cybercriminals who obtain goods from abroad via fraudulent purchases with stolen payment cards. On January 13, 2023, the channel's administrator published an announcement detailing how third-party shipping schemes, which require a network of couriers and a positive relationship with customs officials to execute effectively, were growing in complexity.

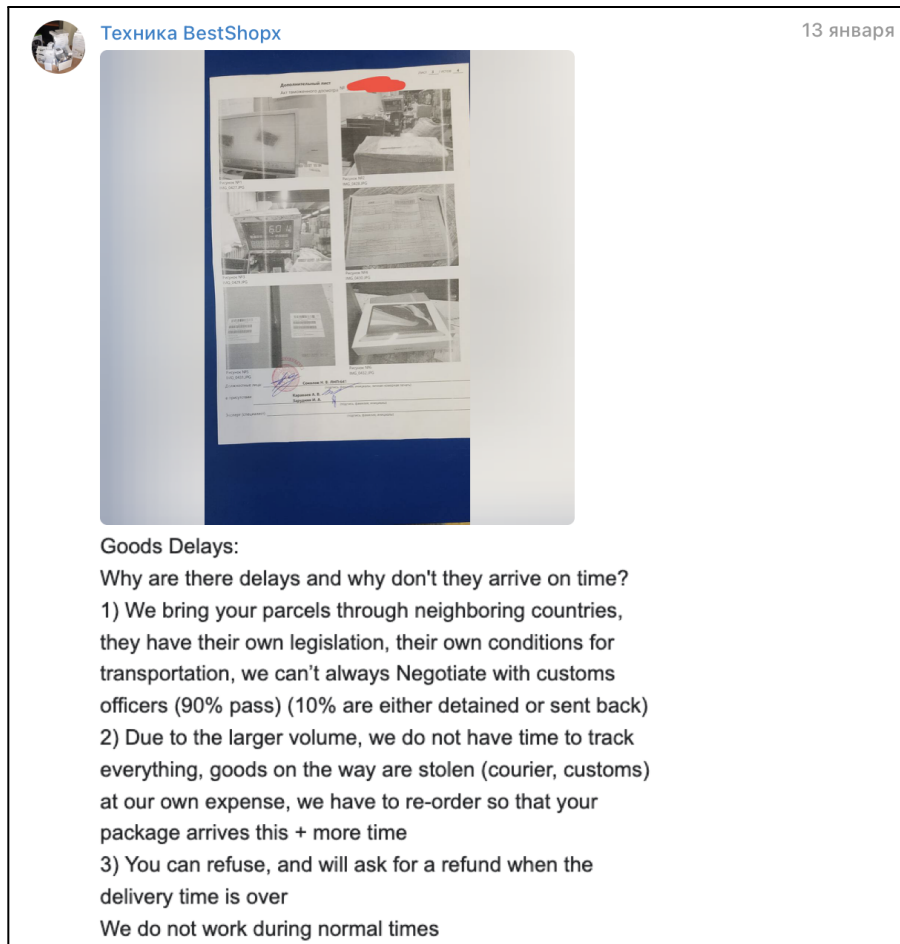



Figure 1: The administrator of an online delivery service explains their current dilemma to their clientele — image text machine-translated from Russian using Google Translate (Source: Telegram)

Insofar as they relate to sanctions evasion, authorities have increasingly caught on to these schemes. In June 2022, a joint FinCEN-BIS alert enumerated a list of transshipment points through which restricted exports had been known to pass before reaching Russian buyers. In May 2022, Kazakhstan [tightened](#) regulations for issuing payment cards to Russian citizens to reduce the risk of Kazakh banks falling under secondary sanctions.

One viable alternative to foreign-issued payment cards is prepaid cryptocurrency virtual credit cards (VCCs). Many Russian freelancers, IT professionals, and criminals already receive direct payment in cryptocurrency, and other Russian entities can make use of third-party services to swiftly convert their rubles into cryptocurrency. Cryptocurrency VCCs subsequently convert these crypto assets into US dollars (USD) to conduct purchases with US merchants that would otherwise be impossible.

On September 29, 2022, the threat actor "razmah" on the dark web forum Exploit inquired about online payment methods for Russian residents. In particular, they expressed interest in anonymous prepaid cards that could be funded using cryptocurrency. On October 2, 2022, the threat actor "tired" replied and suggested an online crypto service that issues prepaid cryptocurrency VCCs.




Prepaid, rechargeable VISA cards. Where ?

By razmah, September 29, 2022 in Other

Follow 3

Start new topic

Reply to this topic



razmah
petabytes
●●●●●●

User
+18
461 posts
Joined
11/29/10 (ID: 34564)
Activity
other

Posted September 29, 2022

Report post

there used to be a theme of prepaid cards. there were sellers who gave a number and you replenish through the seller, are there any now?


Are there any cards that you can replenish yourself? USDT->VISA CARD on the bestchanger for example.

we need anonymous cards with a long validity period. and to work from any country, any name, etc...

well, a survey, to the heap, how do you now pay on the Internet from Russia?

PS I saw such a service like open in your name (on your docks) in Kazakhstan or Armenia. this doesn't fit. firstly, it is not anonymous, secondly, it is tied to a country and a name, otherwise it is a declaring.

+ Quote




tired
kilobyte
●●

User
+12
45 posts
Joined
12/18/17 (ID: 84325)
Activity
другое / other

Posted October 2, 2022

Report post

To pay for services, 
Shops do not accept these cards.

+ Quote

Figures 2, 3: Replying to razmah's inquiry, tired recommended a prepaid cryptocurrency VCC service — image text machine-translated from Russian using Google Translate (Source: Exploit forum)

The same services that threat actors recommend to their peers also provide ordinary Russian consumers with the means to order goods from abroad in defiance of international sanctions. The service recommended by "tired" offers users access to a major card network's prepaid virtual credit cards (VCC). Users convert their rubles to cryptocurrency, which they then use to purchase a VCC from the service. According to the service's website, these VCCs convert the loaded cryptocurrency to USD and are accepted wherever the card network's payment cards are accepted across the US. Importantly, cards can be loaded with a maximum of \$1,000 and do not require user verification.


Recorded Future created a VCC using the service described above. The bank identification number (BIN) displayed on the VCC reveals that the card is issued by a US-based financial institution. A multitude of services provide access to prepaid cryptocurrency VCCs. For the most part, identity verification for the issuance of these cards beneath a certain USD value is either minimal or non-existent. This lack of verification indicates that these card services can be used for illegal ends, including sanctions evasion.

Sanctioned Goods Reach Russia Through Mail Forwarders

Once goods are purchased, they must be delivered. Russian entities make use of mail forwarders, also known as “reshippers”, to obtain goods that are not subject to sanctions. It is likely they do the same to circumvent export controls. Once Russian buyers have obtained a usable payment card, their purchases abroad can be delivered to reshippers’ tax-free warehouses to be repackaged and delivered to Russia.

On April 5, 2022, the threat actor “Mursik” on the dark web forum Slivup requested advice for completing purchases on international websites from Russia. On April 20, 2022, the threat actor “Voron15” recommended a US-based mail forwarder that caters to international customers, which they claimed continued to accept high-technology consumer electronics (such as laptops, tablets, and computer parts) for delivery.

OFF
Mursik
#1




Submitted 05 April 2022 - 05:38

Greetings! Does anyone know how to buy on foreign sites through bank cards if they do not accept from Russia? Maybe there are some services. life hacks, detours?

Platinum
Posts: 262
Registration: 23.04.2014
Earned: 58 rubles

OFF
Voron15
#3



Sent on 20 April 2022 - 16:33

I can share my actual experience on the topic. I have been shopping overseas for 9 years. Current events have left their mark, but everything works.

1. For purchases I use a virtual card [redacted]. I replenish without commission with USDt (on the card they become the equivalent of a dollar). After registering on the service, be sure to verify through [redacted]. And then people are sometimes surprised that the money does not go into the account and God knows how long it takes to return back. In the rules of the service, it is indicated that they have the right NOT to accept payments from unverified accounts. From the moment of replenishment of the account to crediting, it takes an average of 2.5 days, keep in mind (they write at home - that 72 hours for crediting). The card has a business status. I understood this after I tied it to an [redacted] account and he sent me an invitation to their business program. I paid for [redacted] - it goes everywhere without problems.

2. Delivery through an intermediary. You have to be in the moment here. Now there are no equally good ones. For example, [redacted] is one of the most cost-effective, BUT it has stopped carrying equipment and electronics at all for the time being. [redacted] is one of the most expensive, BUT, for example, it still takes equipment for transportation. In general, it is necessary to clarify each time in the caliper.

Platinum
Posts: 8
Registration: 08/05/2021
Earned: 7 rub.
Reputation : 7
Awards: 5

Figures 4, 5: In response to Mursik's inquiry, Voron15 suggested a mail forwarding service for delivering advanced products purchased from abroad — image text machine-translated from Russian using Google Translate (Source: Slivup forum)

Using prepaid VCCs obtained from the crypto services detailed above, patrons can order goods from abroad, which will then be delivered to the “personal address” assigned by the service to users. As a convenient alternative, users can request “purchase assistance” from this mail-forwarding service, which will organize the purchase in exchange for a commission — buyers can compensate the service for these purchases using funds in their account, cryptocurrency, or Russian-issued payment cards.

Either way, once the purchase has been made, the mail-forwarding company receives, logs, and stores delivered packages in its tax-free warehouse, which can be monitored by the buyer. When the buyer is ready, they initiate delivery to Russia, and a shipping fee is deducted from their account balance.

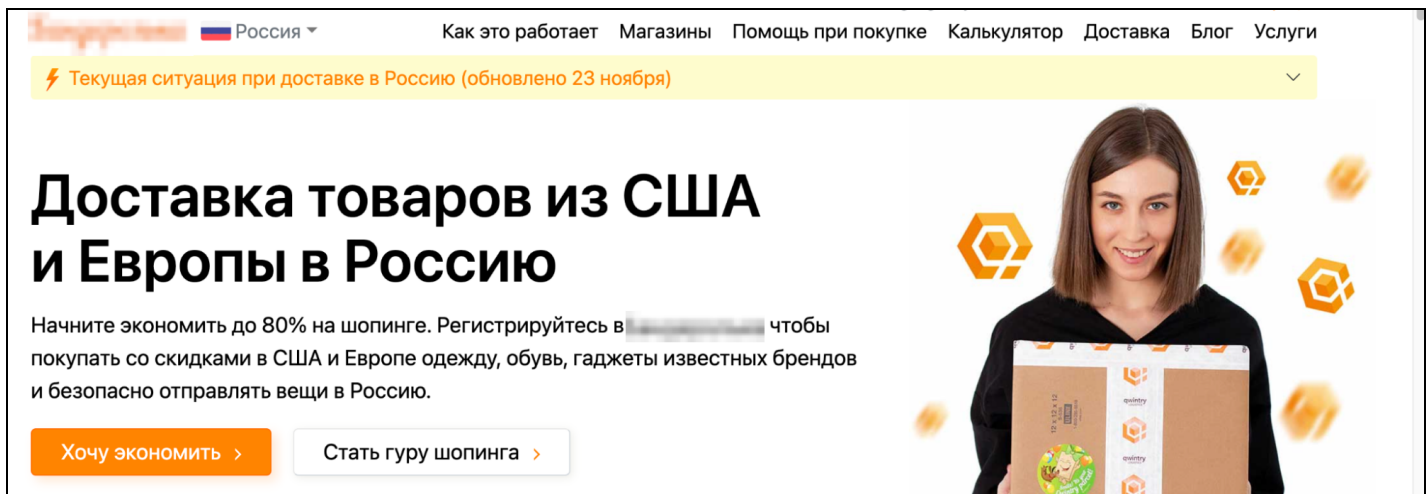


Figure 6: This mail forwarding service advertises “the delivery of goods from the USA and Europe to Russia” and also offers users purchase assistance for goods produced abroad (Source: obfuscated)

As with cryptocurrency payment card services, a host of other popular reshippers exist. Although reshippers publish lists of restricted goods that they are not able to ship to Russia or advisories for unrestricted goods which may nevertheless complicate delivery during customs inspections, the possibility exists that these mail forwarders are used to obtain restricted exports in violation of international sanctions.

Lack of Verification Exposes Financial Institutions and Merchants to Abuse

Financial institutions and merchants are enlisted as unwitting participants in the workarounds described in this report, which is chiefly accomplished due to lack of verification. Non-Russian financial institutions that issue prepaid cryptocurrency VCCs do not verify their clients’ identities under certain dollar thresholds. As a result, they have no way of knowing whether cardholders are on sanctions lists or live in territories subject to export controls. In a similar manner, without verifying their customers’ identities, non-Russian merchants may facilitate the purchase of restricted luxury goods that ultimately reach proscribed Russian markets.

Verification is not a perfect solution. On dark web forums and Telegram channels, cybercriminals pay for fraudulent registration and verification services for crypto exchange accounts, or purchase the stolen personally identifiable information (PII) necessary to fraudulently create verified accounts themselves. In turn, these verified accounts can be used to facilitate various illegal activities, including sanctions evasion. However, more rigorous verification would complicate the workarounds described in this report, likely reducing their use for sanctions evasion by ordinary Russian consumers.

Ultimately, financial institutions and merchants used in these workarounds may be exposed to the risk of secondary sanctions, especially as the workarounds grow more common. In March 2022, US Department of the Treasury Deputy Secretary Wally Adeyemo [threatened](#) secondary sanctions for, among others, financial institutions and [crypto exchanges](#) that helped Russia evade US sanctions. In September 2022, US senators from both the Democratic and Republican parties [expressed](#) interest in punitive sanctions aimed at entities involved in business deals for Russian oil products that sold above a price cap that was later imposed by G7 countries. It is highly likely that this regulatory sentiment extends to the enforcement of sanctions across all spheres.

Mitigations

- Establish more rigorous anti-money laundering (AML) and know your customer (KYC) requirements for issuing cryptocurrency payment cards.
- Monitor transactions and purchases for red flags that suggest they could be involved in sanctions evasion. A detailed list of transactional and behavioral red flags can be found in [FIN-2022-Alert003](#), a FinCEN and BIS Joint Alert published on June 28, 2022.
- For merchants, investigate irregularities in purchases and orders. Unusual order volumes, irregular shipping addresses, and inconsistencies in buying habits may signal that an order or purchase is being made to facilitate parallel imports or sanctions evasion.

Outlook

It is highly likely that as long as Russia's unprovoked full-scale invasion of Ukraine continues, so too will international sanctions. Likewise, as long as international sanctions against Russia remain in effect, Russia will continue seeking new ways to evade them in order to support its war effort, and Russians will search for new means of circumventing them. Workarounds such as prepaid cryptocurrency VCCs and mail forwarding services currently provide Russian consumers with the means to bypass current international sanctions against Russia. Financial institutions and merchants enlisted as unwitting participants in these schemes will continue to be abused until more rigorous verification measures are instituted for the services used to bypass sanctions, including cryptocurrency VCCs and mail forwarding services.

About Insikt Group®

Insikt Group is Recorded Future's threat research division, comprising analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence on a range of cyber and geopolitical threats that reduces risk for clients, enables tangible outcomes, and prevents business disruption. Coverage areas include research on state-sponsored threat groups; financially-motivated threat actors on the darknet and criminal underground; newly emerging malware and attacker infrastructure; strategic geopolitics; and influence operations.

About Recorded Future®

Recorded Future is the world's largest intelligence company. Recorded Future's cloud-based Intelligence Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future provides real-time visibility into the vast digital landscape and empowers clients to take proactive action to disrupt adversaries and keep their people, systems, and infrastructure safe. Headquartered in Boston with offices and employees around the world, Recorded Future works with more than 1,500 businesses and government organizations across more than 60 countries.

Learn more at recordedfuture.com and follow us on Twitter at @RecordedFuture