NISOS

THREAT ANALYSIS

Chargeback Dispute Abuse

How Scam Networks are Defrauding Financial Institutions and Their Customers

September 2023

RESEARCH

Table of Contents

DISCLAIMER:

The reporting contained herein from the Nisos research organization consists of analysis reflecting assessments of probability and levels of confidence and should not necessarily be construed as fact. All content is provided on an as-is basis and does not constitute professional advice, and its accuracy reflects the reliability, timeliness, authority, and relevancy of the sourcing underlying those analytic assessments.

Executive Summary

Nisos researchers identified scamming networks operating thousands of fraudulent online storefronts. The scamming networks use stolen or illegitimately acquired credit cards to make purchases that appear associated with these fraudulent online storefronts. In the instances when a victim whose credit card information was compromised identifies and disputes the fraudulent charges, the websites and shell companies serve as evidence of the store's 'legitimacy' during arbitration by financial institutions. These storefronts lack the infrastructure to actually complete any type of online purchase and exist solely to serve as adequate backstopping during investigations.

Discussions with victims demonstrated that the presence of the fraudulent online storefront and their associated shell companies were sufficient for victims to lose their chargeback disputes, even when the evidence provided by the shell companies was incomplete and inadequate to verify that an actual purchase had taken place. Many financial institutions are under-equipped, facing deluges of chargeback disputes, or require only minimal and easily forged evidence to prove a transaction. This could limit the amount of time, resources, and due diligence that they are able to devote to a single chargeback claim. ***Scamming networks are successfully taking advantage of financial institutions' vetting practices and regulation requirements through this process, which is costing them and the victims of fraudulent transactions significant sums of money.***

Nisos regularly works with local and federal law enforcement agencies to facilitate action against threat actors and e-criminals and can do the same with our clients.

Chargebacks and Chargeback Representation

Consumers can legally dispute charges if they are charged twice for the same item or are billed for merchandise they never ordered, never received, or already returned.[1] [2] In these instances, the bank takes the consumer at their word and reverses the payment, taking the money from the merchant and returning it to the consumer. This is called a chargeback. Unlike a refund, which is provided by the retailer, a chargeback is a reversal of a credit card payment that's issued directly from the bank.

This trust in the consumer is subject to abuse. Anyone can claim to have not made a purchase, dispute the transaction, and create financial hardship for merchants. To combat this, banks have created a process called **chargeback representation**, also known as **chargeback dispute**. Through this process, a merchant can resubmit disputed charges supported by a chargeback rebuttal letter (or a chargeback adjustment request) that includes evidence of the purchase.

The process for submitting chargeback representation requests varies from one financial institution to another. This creates a confusing and complicated situation that can be particularly difficult for smaller merchants.

Tools and services have emerged to facilitate automation of responses to financial institutions. Many of these companies provide a dashboard for merchants to link up their sites and associated transaction

[1]https://consumer.ftc[.]gov/articles/using-credit-cards-disputing-charges
[2]https://consumer.ftc[.]gov/articles/online-shopping#pay

logs, in order to ease the process of chargeback representation when the need arises. Services such as Chargebacks911, Chargeflow, and Midigator are part of a burgeoning industry in chargeback representation automation.

Financial institutions may be aware of these dashboards and believe that they help identify and prevent scams against merchants. They may be unaware that these tools can be utilized by fraudulent merchants to provide forged evidence of stolen transactions. Banks and merchants are likely focused on the high cost that fraudulent chargebacks are putting on their companies, which cost merchants over $20 billion in 2021[3] with fraud costs expected to significantly rise throughout 2023.[4] However, chargeback resolution fraud perpetrated by fraudulent online storefronts is also costing individuals and financial institutions significant money, time, and resources when false charges are unsuccessfully disputed.

Recommendations

Nisos recommends that all credit card holders do their part to combat fraud by vigilantly reviewing bank statements to identify any unattributable charges. In the event a consumer identifies fraud, we recommend that these transaction details be reported to the victim's financial institution. In the event of a chargeback dispute, review the proof of purchase provided by the merchant to the arbitrating financial institutions to ensure that the data it contains is relevant to the claimed charges.

Nisos recommends financial institution investigators look for specific indicators of fraudulent companies when researching chargeback disputes, which include steps such as those outlined below:

1. Collect any contact information available on the website associated with the company (i.e. its associated company name, phone number, email address, physical address, and return address).

2. Search online for these pieces of information — with and without quotes around the search term — in order to identify similar websites and patterns.

3. If product prices listed on these sites are too good to be true, they probably are. This could suggest that actual merchandise is not sold on these sites. A comparison of these products with other online sellers can create a strong baseline for reasonable retail pricing.

4. Verify if the site is able to complete financial transactions, such as by attempting a transaction using a secure and personally-unaffiliated card. In many cases, the storefronts serve only as a facade to legitimize the validity of the store, but cannot actually process a transaction.

5. Verify if the addresses listed for the companies are physical locations or virtual mailboxes through basic online searches and using tools such as Google maps.

6. Consider interacting with the website's support phone number. Scam sites will often rely on what customer service representatives self-refer to as "third-party customer service centers"

[3]https://www.juniperresearch[.]com/whitepapers/fighting-online-payment-fraud-in-2022-beyond
[4]https://www.simplfulfillment[.]com/blog/chargebacks-affect-merchants

and will be unwilling to provide any identifying information about the questionable website or about the call center itself.

7. Carefully review the documentation provided by the suspected fraudulent merchant to the financial institutions for inconsistencies with the alleged charges. Documents with unassociated screenshots and incorrect purchase information have passed financial institutions' vetting processes, causing victims to lose their disputes.

Nisos recommends financial institutions monitor the frequency of total chargebacks, resolved chargebacks, and unresolved chargebacks. While a sudden increase in the number of total or resolved chargebacks may not be due to an increase in scam activity, it does merit a review of the entities involved to determine the legitimacy of business processes.

Scamming Methodology

Scamming networks used the following methods to establish associated fraudulent online storefronts. Other scamming networks beyond the scope of this report likely adopt these practices in whole or in part.

1. **Establishing Shell Companies:** The group overseeing the scamming network utilizes a multi-level marketing (MLM) process to recruit hundreds of otherwise unconnected individuals to establish one or more shell companies with associated bank accounts. The overseeing organization pays the shell company owners for use of the shell company.

2. **Recruiting Scammers:** The overseeing organization controls the shell company and its financials, requiring little effort on the part of the shell company owners. Shell company owners can also recruit additional individuals to set up shell companies, likely receiving financial incentives in the process.

3. **Setting Up Virtual Locations:** The overseeing network instructs shell company owners to use virtual mailboxes and PO Boxes for their business addresses. They use fulfillment centers as their return address, with hundreds of fraudulent online storefronts claiming the same handful of locations.

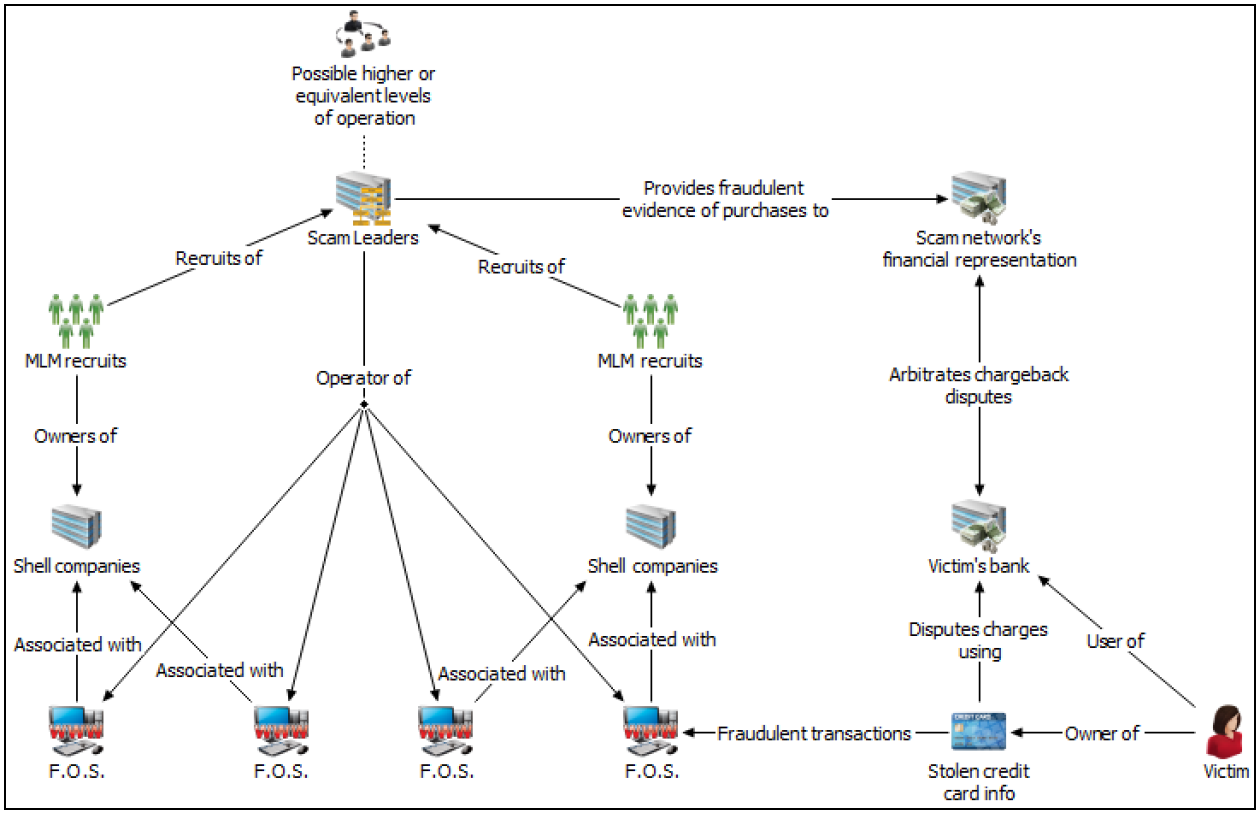
4. **Creating Digital Storefronts:** The overseeing network establishes multiple fraudulent online storefronts and associates them with the shell companies registered by the recruited individuals. The online storefronts do not allow for actual purchases, but serve to add credibility to the company and the fraudulent charges.

5. **Processing Payments:** The scammers use stolen or other illegitimately acquired credit cards to "purchase" items from the fraudulent online storefronts.

6. **Defending Validity:** If a victim identifies and disputes a fraudulent purchase, the infrastructure of the online storefront and the overseeing network at large is able to stand up to most cursory levels of scrutiny and win the chargeback dispute.

This process continually requires new recruits to set up new shell companies for fraudulent websites. These online storefronts generally only survive for up to a year before the number of chargeback claims requires the site to be taken down to avoid suspicion and additional scrutiny.

In our research, we found that many individuals recruited to establish shell companies for these scams owned additional, legitimate businesses. While their social media and other sites advertised these businesses, none of them included any references to the shell companies associated with the scams. This suggests that networks operating fraudulent online storefronts likely seek out or prefer their candidates to be involved in other businesses to appear more legitimate.



Graphic 1: Representation of scam network infrastructure. F.O.S. stands for fraudulent online storefronts.

Chargebacks in Context of the Scamming Network

Scamming networks likely use stolen credit cards to make purchases on fraudulent online storefronts associated with their network. If a victim identifies the fraudulent charges on their card and disputes it through their bank, these sites and associated shell companies have created adequate infrastructure to appear unique and legitimate.

In this context, they will be able to "prove" to the banks that the purchases are real and will likely win the financial dispute. This not only causes financial harm to the initial victim, but has now cost the bank time and resources while also leading them to the incorrect conclusion. The addition of these dashboards further enables scammers to more easily scale their operations. Financial institutions have been caught off guard by an onslaught of automated chargeback representation.

Paperwork for chargebacks and taxes associated with the shell companies are handled by the overarching scam organization. The network likely maintains a centralized operation ready to provide fraudulent documentation to "prove" the validity of a disputed transaction and provide the minimal information required to win the dispute. Our research into networks perpetrating these scams identified purchase validation documents provided by these shell companies that included missing and incorrect data, yet were accepted by the financial institutions as sufficient evidence.

How Scammers Game the System

Scamming networks involved in this process demonstrate how having just enough infrastructure on these fraudulent online storefronts to appear legitimate at face value — in addition to meeting minimal requirements to "prove" a purchase — can often pass bank investigations into chargeback claims. Financial institutions are increasingly losing money when dealing with chargebacks. Banks must determine if disputed transactions are cases of true fraud — where a fraudster steals a cardholder's payment credentials and uses them to make a purchase — or friendly fraud — where a cardholder disputes a transaction and receives a chargeback based on false claims. In this process, every $1 lost to fraud is costing $4.36 in related expenses such as legal fees and recovery, according to a study by LexisNexis Risk Solutions published in November 2022.[5]

The increasing presence of fraud and its rising cost to financial institutions, both in money lost and in associated fees, can possibly lead to insufficient vetting and research into these claims. Scammers have successfully identified the level of infrastructure and facade that has generally been able to pass inspection, as well as the type of supporting documentation that meets the minimum threshold to "prove" a fraudulent purchase.

Carding Darknet Sites

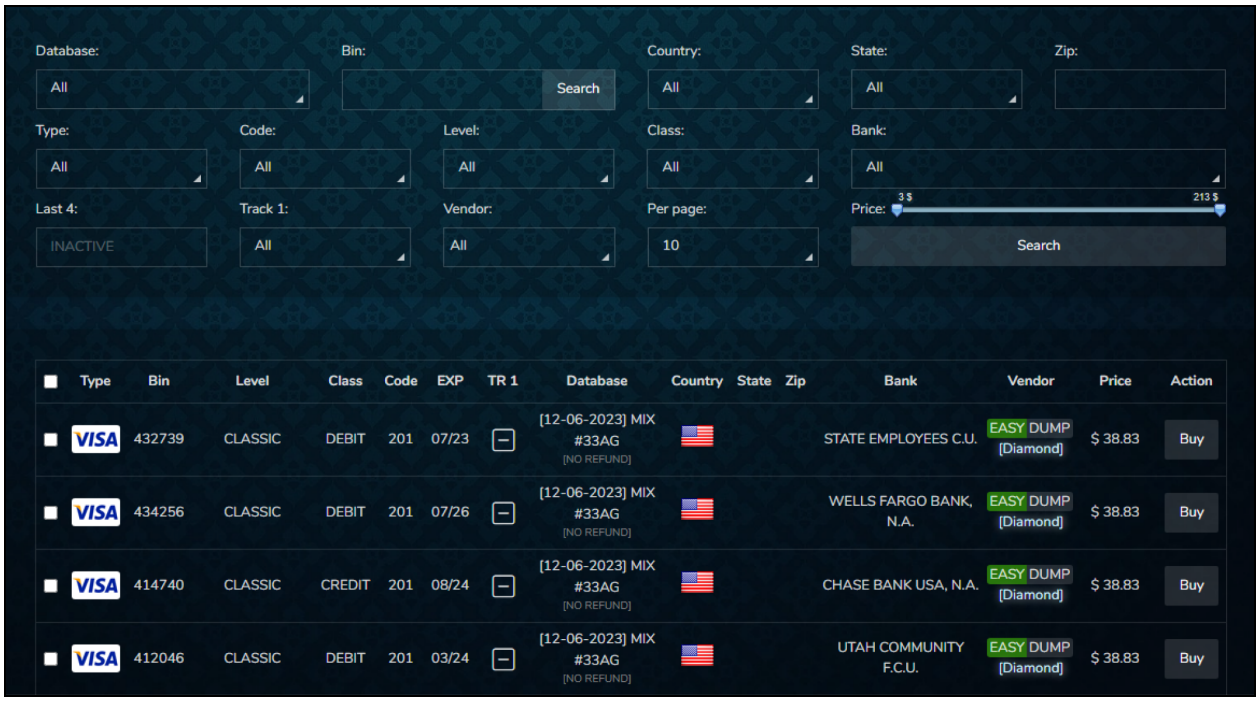
Scammers can easily and cheaply obtain compromised credit card information on a host of deep and dark web marketplaces and forums. Cards sold on these sites enable cyber criminals to conduct unauthorized transactions. Stolen credentials are especially easy for criminals to use in card-not-present (CNP) scams — when the card is not viewed by the merchant for verification, such as online transactions or those conducted over the phone. Reports by Insider Intelligence and LexisNexis project that CNP will make up 74% of fraud by 2024 and estimate that $200 billion will be lost to online payment fraud by 2025.[6] [7]

Threat actors often sell credit card numbers for as little as $7. Card marketplaces generally allow for information to be purchased through Card Verification Value (CVV) and Dump options. CVV purchases include partial or full information about the compromised credit card — generally containing variations of the Bank Identification Number (BIN), credit card number, expiration date, and biographic information for the card owner — providing sufficient data for successful online purchases. Dump purchases contain magnetic strip raw data from the credit card — which can include the associated

[5]https://bankingjournal.aba[.]com/2022/11/survey-finds-fraud-costs-rising-for-banks
[6]https://www.insiderintelligence[.]com/content/spotlight-us-card-payment-fraud-losses-forecast-2022
[7]https://risk.lexisnexis.co[.]uk/insights-resources/article/card-not-present-fraud-in-2022

bank account number, account balance, service code, PIN number, and expiration date — that can enable the data to be used to create a fake card to withdraw money at ATMs.

There are numerous ways that cyber criminals can steal credit card information, including card skimmers,[8] malware, phishing,[9] data breaches, public WiFi network vulnerabilities, or failure to properly dispose of sensitive documents. The increasingly sophisticated and unique ways by which credit card information can be stolen will almost certainly continue to escalate the pressure on financial institutions following customer exposures and required damage mitigation procedures.



Graphic 2: Example of Russian Market credit card batches for sale as of 12 June 2023.[10]

[8]A skimmer is a device installed on card readers that collects card numbers. These can be placed almost anywhere, including ATMs, gas stations, restaurants, or grocery stores. Thieves are generally required to physically retrieve the skimmer to obtain the data stored within.
[9]The fraudulent practice of sending emails pretending to be from reputable companies or individuals to induce individuals to reveal personal information.
[10]http://flydedxmmddhgt3vfhv6om63ra2u2x4jxginulhxb6nzcnj3wwgavwyd[.]onion/dumps

Number	Type	Level	Class	Code	Exp Date	Category	Country	Bank	Action/Result
544212	MASTERCARD	GOLD	CREDIT	606	06/24	New TR1+TR2+PIN	RUSSIAN FEDERATION	COMMERCIAL BANK MASTER-BANK	Buy&Check (30$)
554323	MASTERCARD	STANDARD	DEBIT	606	05/24	New TR1+TR2+PIN	UNITED STATES	FIDELITY INFORMATION SERVICES, INC.	Buy&Check (50$)
437670	VISA		CREDIT	606	05/24	New TR1+TR2+PIN	UNITED STATES		Buy&Check (35$)
416018	VISA		CREDIT	606	07/23	New TR1+TR2+PIN	UNITED KINGDOM	BARCLAYS BANK PLC	Buy&Check (30$)
400336	VISA	CLASSIC	DEBIT	606	05/24	New TR1+TR2+PIN	UNITED STATES	PEAPACK-GLADSTONE BANK	Buy&Check (45$)
528387	MASTERCARD		CREDIT	606	03/25	New TR1+TR2+PIN	JAPAN	UC CARD CO., LTD.	Buy&Check (35$)
584667	MAESTRO	STANDARD	DEBIT	606	06/25	New TR1+TR2+PIN	UNITED STATES		Buy&Check (50$)
422700	VISA		CREDIT	606	08/24	New TR1+TR2+PIN	UNITED STATES	SUMITOMO BANK OF CALIFORNIA	Buy&Check (35$)
438688	VISA	CLASSIC	DEBIT	606	01/24	New TR1+TR2+PIN	UNITED STATES	MERIWEST C.U.	Buy&Check (45$)
413531	VISA		CREDIT	606	08/25	New TR1+TR2+PIN	INDIA		Buy&Check (45$)

Type	Bin	Exp Date	Category	Country	State	City	Zip	Action/Result
VISA	450619	03/2025	Credit Cards	Spain	Madrid	Madrid	"BANKINTER	Buy&Check (7$)
VISA	496663	01/2025	Credit Cards	Spain	Madrid	Madrid	"BANKINTER	Buy&Check (7$)
VISA	450619	12/2023	Credit Cards	Spain	Madrid	Madrid	"BANKINTER	Buy&Check (7$)
VISA	429570	06/2024	Credit Cards	Spain	Madrid	Madrid	"IBERCAIA BANCO	Buy&Check (7$)
VISA	485788	05/2024	Credit Cards	Spain	Madrid	Madrid	POPULAR VISA IBERIA	Buy&Check (7$)
VISA	491804	01/2025	Credit Cards	Spain	Madrid	Madrid	"BANKIA	Buy&Check (7$)
MasterCard	549928	08/2024	Credit Cards	Spain	Madrid	Madrid	"SERVICIOS FINANCIEROS CARREFOUR	Buy&Check (7$)
VISA	403617	09/2023	Credit Cards	Spain	Chiclana De La Frontera	Chiclana De La Frontera	"BANCO COOPERATIVO ESPANOL	Buy&Check (7$)
VISA	459990	03/2025	Credit Cards	Spain	Churriana-Malaga	Churriana-Malaga	"BANKIA	Buy&Check (7$)
VISA	476665	09/2023	Credit Cards	Spain	Gines	Gines	"CAIXABANK	Buy&Check (7$)

Graphics 3 and 4: Example of ltd-cc[.]ws credit card batches for sale as of 12 June 2023.[11]

[11]https://ltd-cc[.]ws/index.php#

Conclusion

Scammers have identified ways to meet the minimal requirements in “proving” fraudulent purchases, which allows them to support themselves with money received from stolen information. The widespread tactics implemented by these scamming networks provide avenues whereby diligent investigation can identify indicators of fraud.

Investigators can use the examples listed throughout this report as indicators of potential fraud when considering their own unique situations. In addition to the examples provided above, Nisos researchers support our clients’ unique needs through investigative support and by sharing with investigative teams its pre-existing understanding of existing chargeback threat actors. To help mitigate further fraud and abuse perpetrated by this scamming network and others, Nisos researchers can also provide training to investigators and arbitrators who handle chargeback disputes regarding fraud indicators and how to research pieces of information that are most likely to reveal a hoax.