CYBER
THREAT
ANALYSIS

Recorded Future®

By Insikt Group®

December 21, 2023

Annual Payment Fraud Intelligence Report: 2023

Executive Summary

Throughout 2023, many indications suggested that the payment fraud underground has begun to recover from Russian law enforcement's crackdown against domestic cybercriminals and the subsequent full-scale Russian invasion of Ukraine in 2022. The volume of cards posted for sale on dark web carding shops has rebounded, and cybercriminals have refined their techniques for stealing funds and data. With 119 million stolen payment cards posted freely or for sale online and a median fraud charge of $79 in 2023, the implications are alarming: the stolen cards we analyzed this year represent $9.4 billion in preventable fraud losses for card issuers and $35 billion in potential chargeback fees for merchants and acquirers. Even more alarming is that fraudsters in 2023 increasingly used refined social engineering tactics (via phishing and scams) and sophisticated cyber-based tools and fraud schemes (such as 3-D Secure [3DS] bypass software and scrupulous new account fraud [NAF] workflows) to bypass rules-based fraud detection programs and enact their fraud schemes.

The 2023 events and fraud trends analyzed in this report offer a glimpse into the payment fraud threat landscape for 2024, which will likely witness a persevering payment fraud underground along with continuing growth in sophisticated, hybrid cyber-fraud threats. These dynamics suggest the trend toward hybrid cyber-fraud threats is likely to accelerate and that financial institutions (FIs), payment processors, merchant services companies, and other stakeholders should allocate business resources accordingly. This can be achieved through increased resource-sharing between cyber threat intelligence (CTI) teams and fraud teams along with the concerted development of specific use cases for CTI-fraud coordination. A primary use case would be establishing an "analytical loop" for collaboration between CTI and fraud teams. For example, fraud team analysis of card activity for payment cards that have suffered fraud events can help identify where the cards were compromised, which can lead to the identification of additional at-risk cards. Subsequent CTI analysis of these likely points of breach may reveal indicators of compromise (IOCs) that CTI and fraud teams can extrapolate for analysis across a broader sample to surface more potential breaches and compromised cards.

This cyber-fraud fusion approach would likely increase the value derived from fraud prevention efforts in exchange for increased operating costs, particularly with regard to implementation. Most stakeholders — particularly FIs — would likely garner net financial benefits from this cyber-fraud fusion approach as a result of improved business outcomes and operational efficiencies. We advance additional use cases in the "Mitigations" section of this report.

Key Findings

- In 2023, we continued to see Magecart actors using Google Tag Manager (GTM), Telegram Messenger, and attack-carrier domains for their e-skimmer infections. Meanwhile, we observed various advancements in the Magecart tactics, techniques, and procedures (TTPs) used to obfuscate e-skimmer infections.
- Our identification of CPPs in 2023 indicated that threat actors continue to target restaurants, bars, and online ordering platforms to breach payment card data while phishing and scam pages gained prominence as a method of card compromise.
- The majority of breaches and Magecart e-skimmer infections we identified in 2023 targeted US merchants, although a substantial portion of Magecart e-skimmer infections also targeted merchants in other countries with developed e-commerce sectors.
- Looking forward to 2024, fraudsters will likely continue to refine their TTPs as they employ "old faithful" methods to compromise cards.
- Throughout 2023, the supply of stolen payment cards posted for sale on dark web carding shops recovered following 2022's system shocks, and stolen cards issued by North American and European financial institutions led the world in the overall volume of cards posted for sale. These trends will likely persist in 2024.
- In 2023, Telegram sources became an increasingly important source of free full card data on the internet, but free card data posted online remained lower-threat than for-sale card data on dark web carding shops. These patterns will likely persist in 2024.
- Threat actor card-testing activity continued to develop and play a key role in the card fraud underground in 2023 — a pattern that will likely persist in 2024.
- Workflows and technical solutions for 3DS bypass gained popularity on cybercriminal sources in 2023.
- In 2023, we observed increasingly sophisticated schemes that allow threat actors to compromise and monetize financial data as part of a fraud-based malvertising ecosystem.
- Information sharing, particularly through detailed guides on cybercriminal sources, likely facilitated new account fraud (NAF) in 2023.
- Cybercriminals in 2023 relied upon Telegram — particularly check fraud channels and Telegram bots with card-testing and generation functionality — to enable their fraud schemes.
- Throughout 2023, cybercriminals developed and employed artificial intelligence (AI) workflows to facilitate fraud schemes following the advent of accessible generative AI in early 2023.
- In 2023, cybercriminals demonstrated increased reliance on social engineering tactics that exploit the unwitting assistance of victims to bypass fraud detection mechanisms entirely.
- Looking forward to 2024, fraudsters will likely continue to combine increasingly sophisticated technical solutions, nuanced workflows, and social engineering tactics to bypass rules-based fraud detection rules.

Table of Contents

Background

Payment fraud occurs in a life cycle (Figure 1). By analyzing the data trends and events related to each stage of this life cycle, stakeholders in the payments ecosystem — including FIs, payment processors, merchant services providers, and others — can gain key insights to mitigate the risk of financial fraud.

1. In the first stage of this life cycle, threat actors steal payment card and cardholder data through **Merchants Compromised** by physical card skimmers, Magecart e-skimmers, or other means of data theft.
2. Next, threat actors post this data for sale, often on **Carding Shops** on the dark web.
3. Sometimes, threat actors release **Free Card Data** and accompanying cardholder data to boost their reputations, promote their criminal offerings, or as an accidental result of poor system configuration.
4. Once "end-user" fraudsters have acquired card and cardholder data, they often check its validity using **Tester Merchants**.
5. Finally, fraudsters attempt to monetize the payment card and cardholder data through a **Fraudulent Transaction Placed** on a merchant's website, targeted or generalized phishing and scam attacks, or by other means.

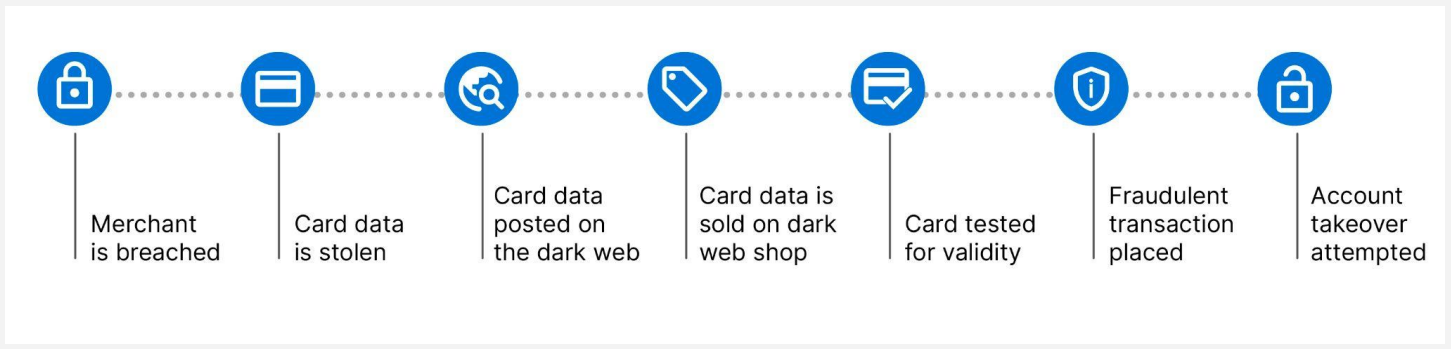


Figure 1: *Payment card data is often stolen, sold, and monetized within a greater fraud life cycle (Source: Recorded Future)*

Methodology

This report is based on an analysis of data from dark web and clearnet sources, including dark web carding shops, dark web marketplaces, dark web forums, dark web card-testing services, Telegram Messenger channels, and open-source reporting. This report also includes proprietary data from Recorded Future's Payment Fraud Intelligence module and Recorded Future's proprietary Magecart e-skimmer scanner, Magecart Overwatch. Transaction analysis used to identify sources of breached data and enriched merchant information for this report was achieved in collaboration with partner FIs. All data analyzed in this report was collected from January 1, 2023, to November 30, 2023.

Threat Analysis

As covered in our previous annual report, 2022 was a year of system shocks. Russia's 2022 cybercrime crackdown and subsequent full-scale invasion of Ukraine early in the year reverberated throughout the card fraud underground. As a result, the volume of payment cards posted for sale on dark web carding shops in 2022 contracted by 38%, shrinking from over 90 million cards in 2021 to under 60 million.

Despite these system shocks, fraudsters demonstrated remarkable adaptability and resilience in the face of adversity throughout 2022:

- Magecart threat actors seized the opportunity to employ novel TTPs with their card-stealing e-skimmer infections.
- Compromises at online ordering platforms for restaurants and ticketing solutions for entertainment and transportation companies allowed cybercriminals to steal cards from multiple merchants with a single breach.
- Carding shops exploited the supply shortage by flooding the market with low-quality payment cards.
- At least one dark web card-testing service systematically incorporated high-profile tester merchants into its infrastructure to validate stolen payment cards and evade detection.

In 2022, we predicted that the future of the payment fraud market in 2023 would remain highly dependent on the outcome of Russia's war in Ukraine. In reality, however, the payment fraud threat landscape of 2023 has demonstrated that threat actors were far more willing to adapt to changing economic conditions than we anticipated, as demonstrated by the following:

- Our analysis this year surfaced **119 million stolen payment cards** posted freely or for sale on various sources online throughout 2023.
- With a median fraud charge of $79 in 2022, these 119 million stolen cards represent **$9.4 billion** in preventable fraud losses for card issuers.
- Additionally, with average fraud costs of $3.75 for each dollar in fraud losses, these potential fraud losses represent **$35 billion** in potential chargeback fees for merchants and acquirers.

This report covers major 2023 fraud trends, updates, and what those findings mean for the payment fraud threat landscape in 2024. We organize this report by the stages of the payment fraud life cycle, beginning with card compromise and ending with the fraud schemes threat actors used to monetize stolen data in 2023.

Merchants Compromised: For Magecart E-skimmer Infections and Other Compromises, Fraudsters Combine New Tricks with Old Tactics

Throughout 2023, threat actors developed their tools and TTPs to combine old methods with new tricks, a trend that will likely continue in 2024. Our proactive analysis in 2023 indicated that Magecart e-skimmer infections remained a mainstay for threat actors seeking to steal payment cards by compromising online e-commerce transactions. At the same time, retroactive transaction analysis conducted in collaboration with partner FIs indicated that payment card records posted for sale on dark web carding shops largely originated from bars, restaurants, and online ordering platforms — historically popular targets for stealing card data.

Magecart E-skimmer Infections Continue to Advance and Primarily Target US Customers

Throughout 2023, Magecart e-skimmer infections remained the premier example of how threat actors enable fraud through cyber TTPs, a trend that is likely to continue in 2024. Magecart e-skimmers collect customer information and payment card data during the e-commerce checkout process, and many e-skimmers replace legitimate payment card data collection forms with a facsimile to bypass payment gateway configurations.

The attack chain for a Magecart e-skimmer infection typically looks as follows:

- Infections are injected directly into resources on a victim website (including HTML, JavaScript, .png files, and more), the server-side code that produces the website's root page, or through URL injection into one of the resources mentioned above, which retrieves the e-skimmer from another source.
- Often, Magecart e-skimmer infections inject a small loader script into the root page of the website, which installs the e-skimmer after the customer navigates to the website's checkout page.
- Afterwards, data theft usually occurs in the e-commerce website customer's browser.
- Finally, threat actors devise means to exfiltrate stolen data from the victim browser to infrastructure under their control.

Magecart merchant infection data offers insight into whether a card is likely to have been compromised before that card is posted for sale on dark web carding shops.

Infection Status	All Infected E-commerce Hosts	Currently Infected E-commerce Websites
Active during 2023, regardless of when the infection occurred	5,700	1,900
First detected during 2023	3,500	1,000

Table 1: *Of all e-commerce hosts that were infected throughout 2023 (regardless of when they were infected), more than half actually became infected in 2023, and around 1 in 3 remain infected as of this writing (Source: Recorded Future)*

Ultimately, we identified multiple Magecart campaigns throughout 2023, each with its own specialized TTPs. Notable 2023 campaigns included *Megaebun, Kritec, Grelos GTM, flex-query,* and *gopay*. Throughout 2023, the primary TTPs used in Magecart infections (for example, payment form replacement, injection of e-skimmer code, and obfuscation of e-skimmer code) remained fairly consistent. We also continued to see Magecart actors using platforms such as Google Tag Manager (GTM), Telegram Messenger, and attack-carrier domains (legitimate websites abused by threat actors) as attack infrastructure. These TTPs are likely to remain widespread in 2024.

Meanwhile, we observed several key advancements that demonstrate Magecart actors continue to refine their TTPs for evading detection, including:

- Multiple logical paths within e-skimmer code, many of which are not executed, for inhibiting reverse engineering (Kritec)
- The use of loader scripts that connect to relay URLs, which respond with the e-skimmer URL for injection into the e-commerce website (Kritec)
- Use of multiple Trojanized GTM containers in a chained loading structure (GrelosGTM)
- Obfuscated object-based e-skimmer structure (Megaebun)
- Abuse of Telegram bot application programming interfaces (APIs) for e-skimmer URL relay and data exfiltration (multiple)

In 2023, the overwhelming majority of infections targeted e-commerce businesses frequented by US customers, part of a historical trend that is likely to continue in 2024. Nevertheless, merchants in other countries with developed e-commerce sectors also faced the risk of e-skimmer infection (Figure 2).

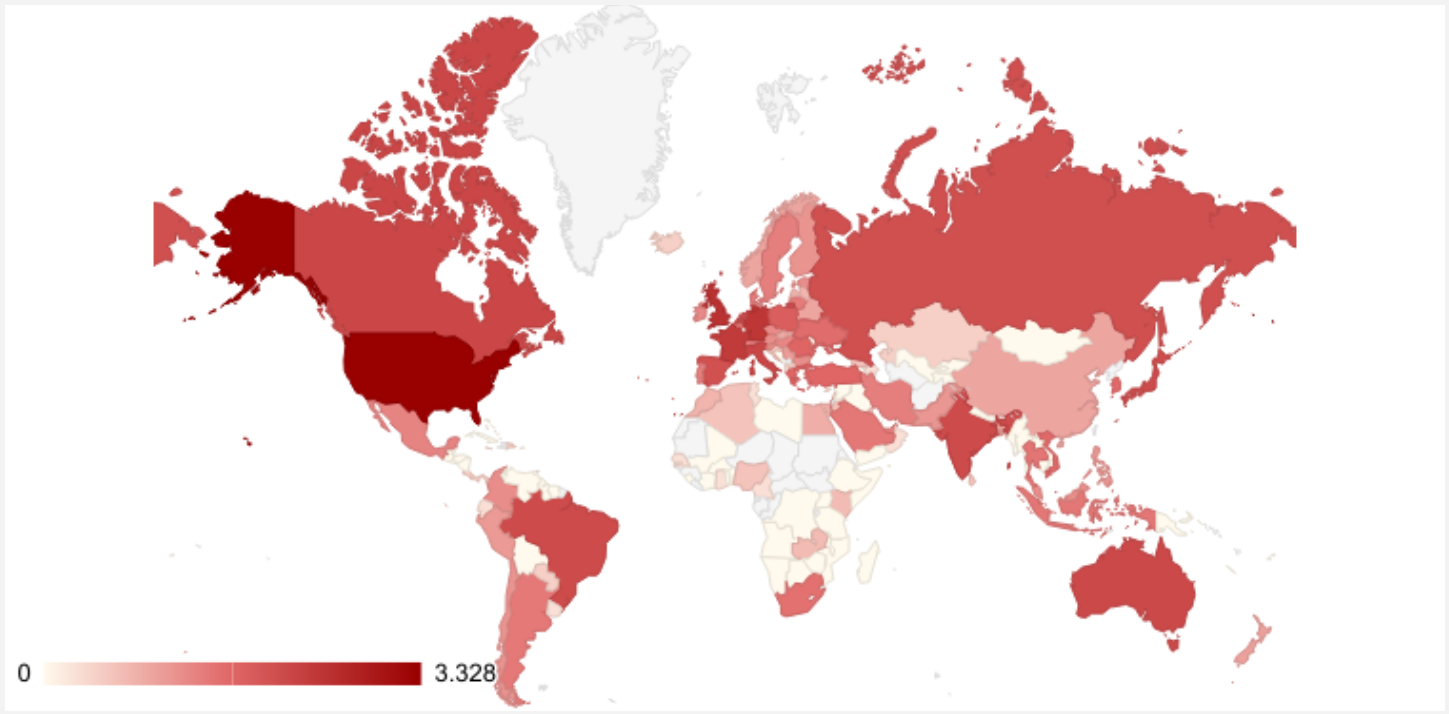


Figure 2: *This map displays the concentrations of e-skimmer infections targeting online e-commerce customers in various countries, with logarithmic values used to enhance contrast. We used e-commerce website traffic data to determine a given e-skimmer infection's target countries. If this data was unavailable, we supplemented the chart with the merchant's domain hosting and business headquarters geodata. (Source: Recorded Future, Similarweb)*

Common Points of Purchase (CPPs): Fraudsters Blend Old and New Methods to Punch Above Their Weight

Throughout 2023, our identification of common points of purchase (CPPs) demonstrated few novel developments, underlining the perennial nature of the threat that card compromise poses to merchants, FIs, and their customers. CPPs — or merchants where multiple compromised cards within a single set have transacted — are often likely to be sources of compromise. To identify CPPs, we collaborate with partner FIs to conduct transaction analysis of payment card records posted for sale on dark web carding shops.

Total Count of CPPs Identified in 2023	CPPs with Attributable Card Records on Dark Web
2,400	1,500

Table 2: *In 2023, we collaborated with partner FIs to attribute for-sale records on dark web carding shops to 2 out of every 3 CPPs identified through transaction analysis (Source: Recorded Future, partner FIs)*

As is typical, the bulk of CPPs we identified in 2023 were US-based merchants, which will likely remain prominent targets for fraudsters in 2024. Figure 3 shows the locations of the CPPs we identified. Blue pins represent CPPs that were linked to CNP data for sale on dark web carding shops, whereas orange pins represent CPPs linked to CP data.

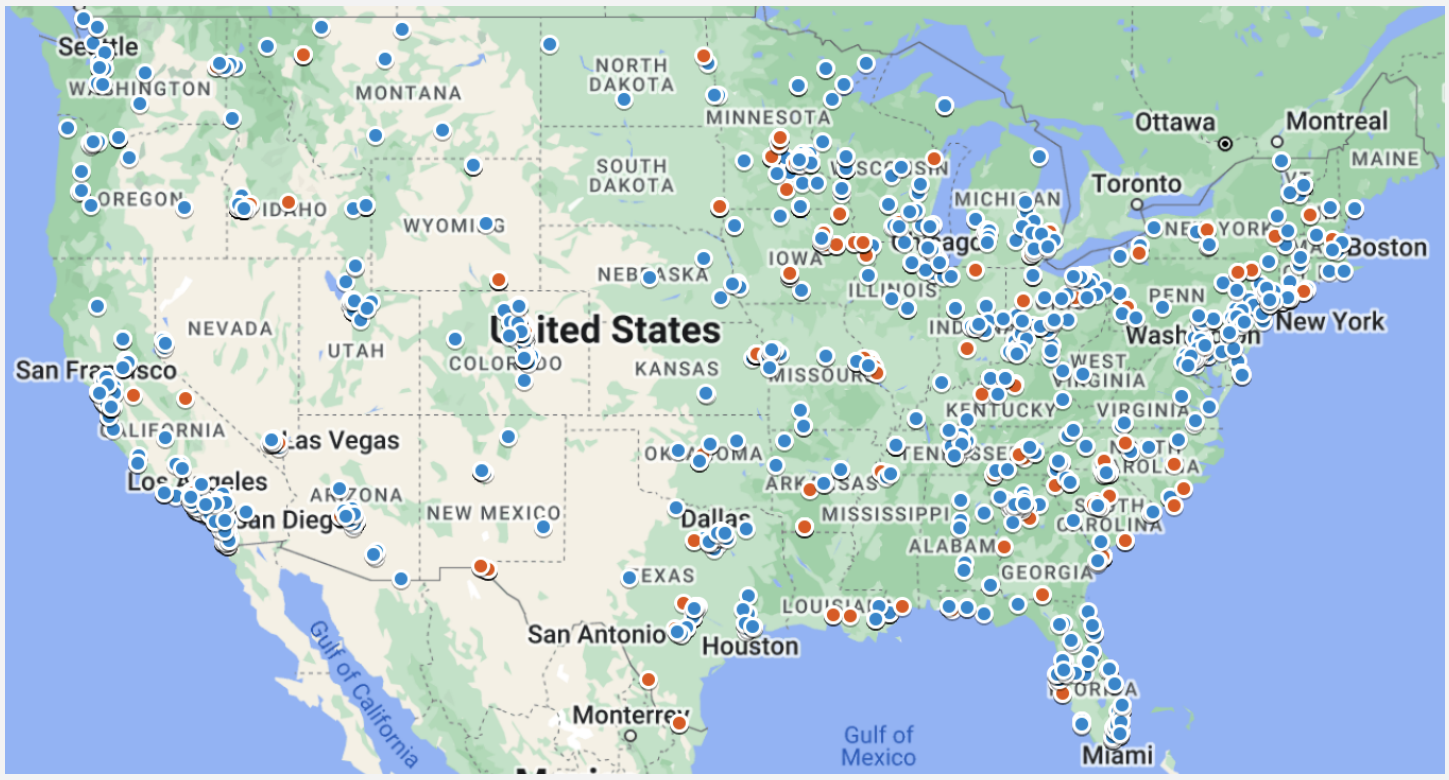


Figure 3: *Orange pins represent the physical location of merchants affected by CP breaches, whereas blue pins represent the headquarters for companies affected by CNP breaches (Source: Recorded Future)*

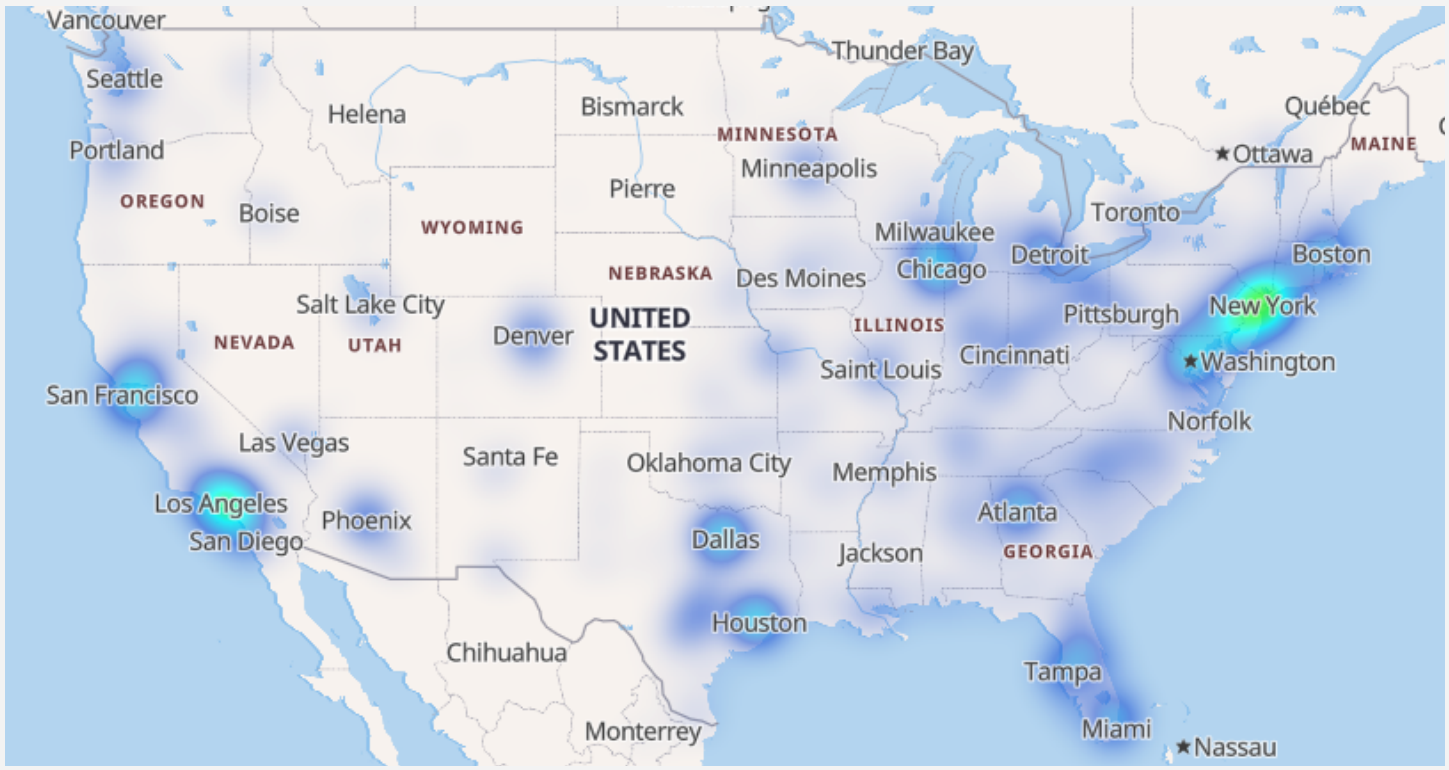


Figure 4: *In 2023, the majority of compromised cards posted for sale on dark web carding shops and attributed to CPPs belonged to US cardholders in major metropolitan areas (Source: Recorded Future, partner FIs)*

Throughout the year, transaction analysis and merchant data enrichment surfaced various patterns in the merchant category codes (MCCs) most frequently associated with CPPs. Of the top 5 most common MCCs among CPPs this year, 5812 ("Eating Places and Restaurants") was far and away the most common MCC. This corresponds to the high frequency of small restaurants and bars among sources of card data in 2023 and previous years, a trend that will likely remain steady going into 2024.

Restaurants and bars in the US remain vulnerable to CP breaches due to their frequent use of centralized point-of-sale (POS) systems. In the US, servers often obtain cards from customers for payment to bring them to the POS and out of the customer's view. This presents unscrupulous staff members with an opportunity to steal the data contained on a card's magstripe using a pocket skimmer.

Top 5 CPP MCCs for 2023	Description
5812	Eating Places and Restaurants
5533	Automotive Parts and Accessories Stores
5691	Men's and Women's Clothing Stores
5999	Miscellaneous and Specialty Retail Stores
5941	Sporting Goods Stores

Table 3: *In 2023, most CPPs we surfaced were associated with the above MCCs (Source: Recorded Future)*

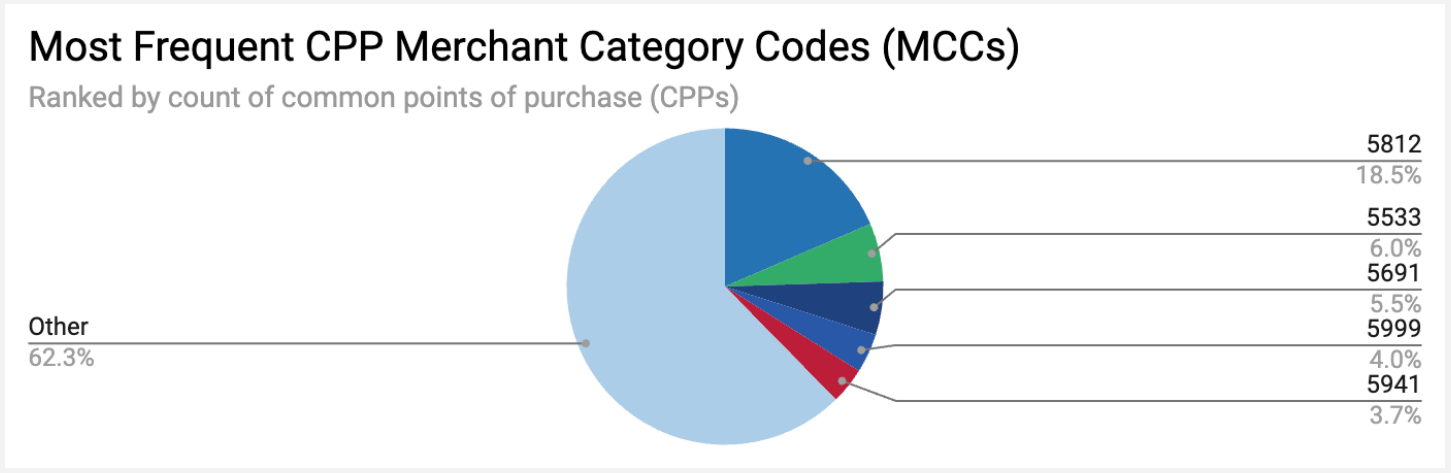


Figure 5: *In 2023, nearly a fifth of the CPPs we surfaced used 1 MCC, and nearly 40% of all CPPs used 1 of 5 MCCs (Source: Recorded Future)*

As restaurants and bars continued to comprise most CP data breaches in 2023, platform breaches allowed threat actors to punch above their weight. By compromising a single online platform, threat actors can potentially compromise transactions with all merchants that make use of the platform. We confirm that merchants identified as CPPs through transaction analysis were breach sources through manual Magecart analysis, and we consider platform breaches likely if Magecart or transaction analysis points to a substantial amount of CPPs using that platform.

Among this year's likely platform breaches, the highest-impact compromises targeted various industry verticals:

- **AudienceView, an online ordering platform for university event tickets,** was targeted by a single Magecart campaign that resulted in e-skimmer infections for 3 unrelated universities using University Tickets. It is highly likely that a significant portion — if not all — of the universities using University Tickets at the time of the breach were exposed to compromise. To date, we have identified 100 universities that used University Tickets for online sales that may have been infected. This campaign began no later than February 14, 2022, and persisted until February 21, 2023. On March 28, 2023, AudienceView confirmed a data breach had affected 13,045 people.
- **An online gift card platform that hosts merchant subdomains** was targeted by a single Magecart campaign that resulted in e-skimmer infections for 59 merchants using the platform. This campaign began no later than March 23, 2023, and persisted until April 24, 2023.
- **An online restaurant ordering platform service** was likely breached by unknown means. Transaction analysis indicated 63 restaurants using the platform were CPPs for cards posted for sale on a single dark web carding shop. These CPPs were likely exposed no later than July 12, 2023, until at least August 4, 2023. We have historically identified online restaurant ordering platforms as common targets for compromise, suggesting that they present favorable targets for threat actors.

Finally, in 2023, we observed a marked increase in the quantity of suspected scam pages among CNP CPPs identified through transaction analysis, suggesting that online scam website campaigns will present a growing threat throughout 2024. Unlike traditionally compromised e-commerce merchants, scam websites are purpose-built to steal card data through online payments or phishing tactics. Often, victims receive bogus or low-quality goods or nothing at all after submitting their payment data.

In 2023, several high-impact scam website campaigns, including those listed below, suggest that 2024 will bear witness to an increased threat of card compromise and financial theft via scam and phishing pages:

- A subscription scam campaign consisting of no fewer than 348 domains
- Various cryptocurrency scams that combine cryptocurrency drainers with phishing tactics to steal victims' crypto assets
- A smishing campaign that distributed text messages containing links to scam pages modeled after the websites of the US Postal Service (USPS) and other nations' postal services, which likely resulted in the compromise of at least 35,000 card records and possibly as many as 400,000
- A network of 201 scam domains likely operated by the same threat actor(s)

Carding Shop Data: As Full-Scale War in Ukraine Approaches Third Year, Volumes of Stolen Card Data on Carding Shops Recover from 2022 Low

In 2023, for-sale card records presented a higher fraud threat than card records posted for free. In 2023, cards issued by at least 10,000 FIs across the globe were offered for sale in the carding shops we analyzed. The quality of for-sale card records tends to vary by carding shop, but for-sale card data almost universally belongs to higher threat segments than free card data posted to online sources.

Carding Shop Data: Trends and Updates

In 2023, threat actors posted higher volumes of stolen credit cards for sale on dark web carding shops compared to 2022, indicating that the dark web fraud ecosystem has rebounded from the initial system shocks caused by Russia's 2022 law enforcement crackdown and subsequent full-scale invasion of Ukraine. Barring additional unforeseen system shocks, this recovery will likely continue in 2024. Ultimately, the ongoing recovery of stolen card data volumes demonstrates the adaptability of fraudsters, who tend to remain adaptive and resilient in the face of adversity.

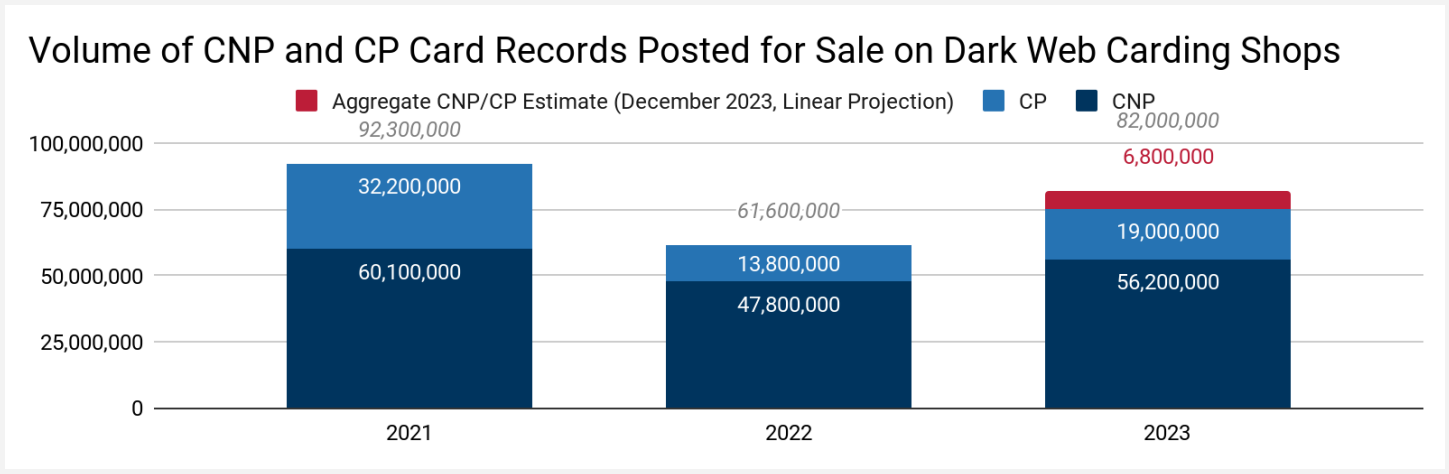


Figure 6: *In 2023, the volume of stolen cards posted for sale on dark web carding shops recovered from 2022's low but remained below 2021 figures (Source: Recorded Future)*

In 2023, we began analyzing stolen card records posted for sale from 10 new dark web carding shops in addition to those we have historically analyzed. Many of these sources were created to fill market vacuums spawned during Russia's 2022 law enforcement crackdown in the lead-up to Russia's full-scale invasion of Ukraine, and their establishment also points to a recovering card fraud underground.

Carding Shop Tier (Cards Posted for Sale Each Year)	Count of New Carding Shops Analyzed in 2023

Low tier (500,000 or fewer)	**6**
Mid tier (500,000 to 2 million)	**3**
Top tier (2 million cards or more)	**1**

Table 4: *In 2023, we began analyzing CNP and CP records posted for sale on 10 new carding shops, many of which were created throughout 2022 and 2023 to fill market vacuums as part of an ongoing recovery (Source: Recorded Future)*

Despite the multitude of 2023 carding shop openings, in July 2023, a single mid-tier CNP carding shop announced its closure for the second time. Previously, this carding shop opened in April 2022, closed in late September 2022, and reopened in April 2023. Our analysis indicates this carding shop's operators likely earned $300,000 in revenue following its reopening. The closure of this relatively minor marketplace with low card volumes had no substantial impact on the stolen card data market at large.

Carding Shop Metrics: 2023 Supply and Pricing Dynamics

The supply of CNP and CP records posted for sale on carding shops in 2023 increased to 71.4 million records, up from 60 million in 2022 — for fraudsters, likely a positive sign going into 2024. The median price of CP records remained stable as the median CNP record price increased from $8.55 to $12.00 per record, demonstrating growing perceived value for those records in aggregate (although to some degree, median price growth from 2022 to 2023 may have been distorted by high inflation throughout 2022). In keeping with historical trends, CNP records posted for sale in 2023 vastly outnumbered CP records. Altogether, our analysis indicates that cards issued by at least 10,000 banks across the world were compromised in 2023.

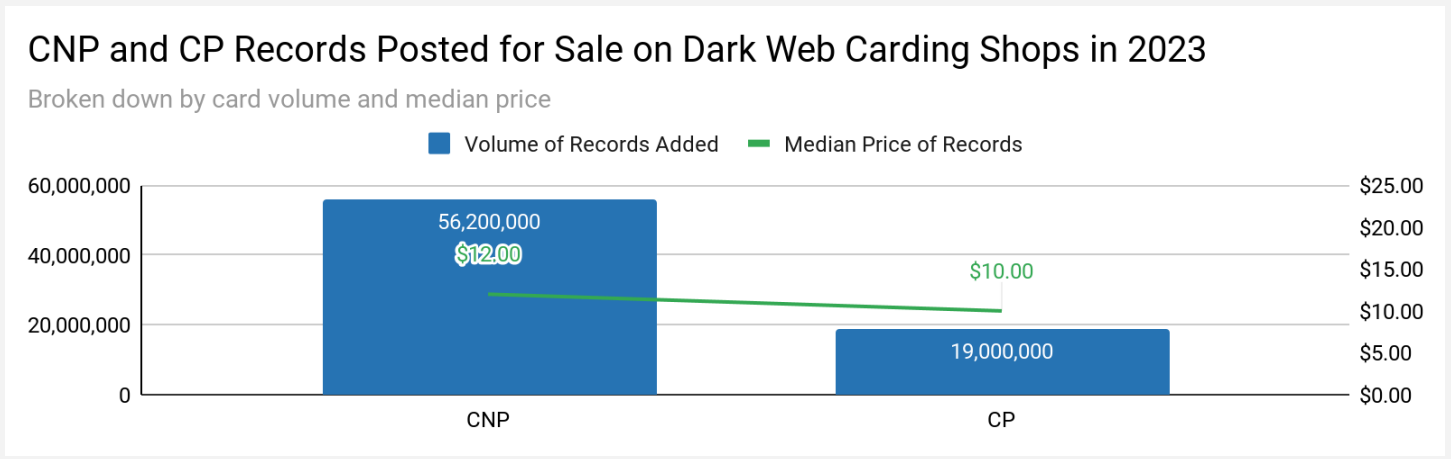
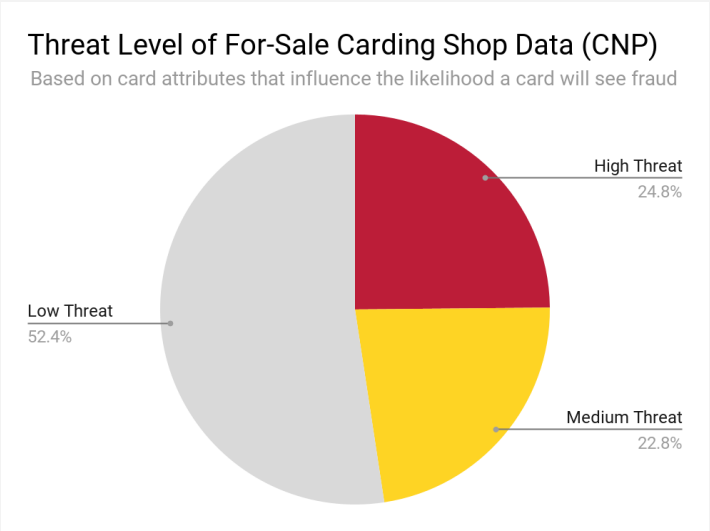


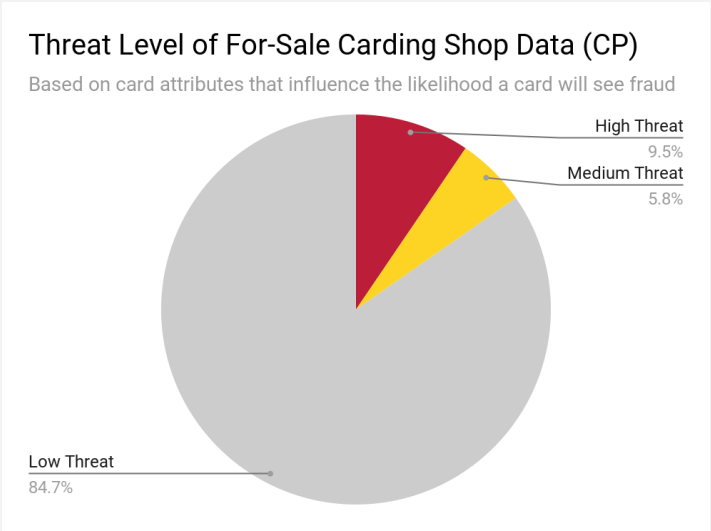
Figure 7: *In 2023, the volume and median price of CNP records posted for sale on carding shops exceeded those of CP records, indicating that threat actors continue to prefer CNP records for fraud (Source: Recorded Future)*

In 2023, CNP card records posted for sale on carding shops generally belonged to higher threat segments than CP card data, indicating that CNP card records likely face a higher fraud threat than CP records. This dynamic is a mirror reflection of fraudsters' preference for CNP data over CP data over the

past 5 years. This preference is likely the result of a range of factors, including improving physical card security measures (exemplified in EMV chip cards and near-field communication [NFT] payment methods) and the surging popularity of e-commerce transactions, which was accelerated by the COVID-19 pandemic.

We developed threat segmentation for card data on the dark web and other sources based on certain criteria that influence whether a given card is more or less likely to see a fraud event. We identified these criteria based on internal analytics and proprietary fraud data. High threat-level card segments are more likely to see fraud events, whereas low threat-level card segments are less likely to see fraud events.





Figures 8 and 9: *In 2023, CNP card records for sale on carding shops generally belonged to higher threat segments than CP records (Source: Recorded Future Intelligence Cloud)*

In 2023, the quantity of cardholder PII available for purchase with for-sale card records on dark web carding shops predictably increased across the board. Similarly, in 2024, the availability of PII with stolen card records will likely be a function of the total card records available for sale. Fraudsters often use accompanying cardholder PII to support various fraud schemes.

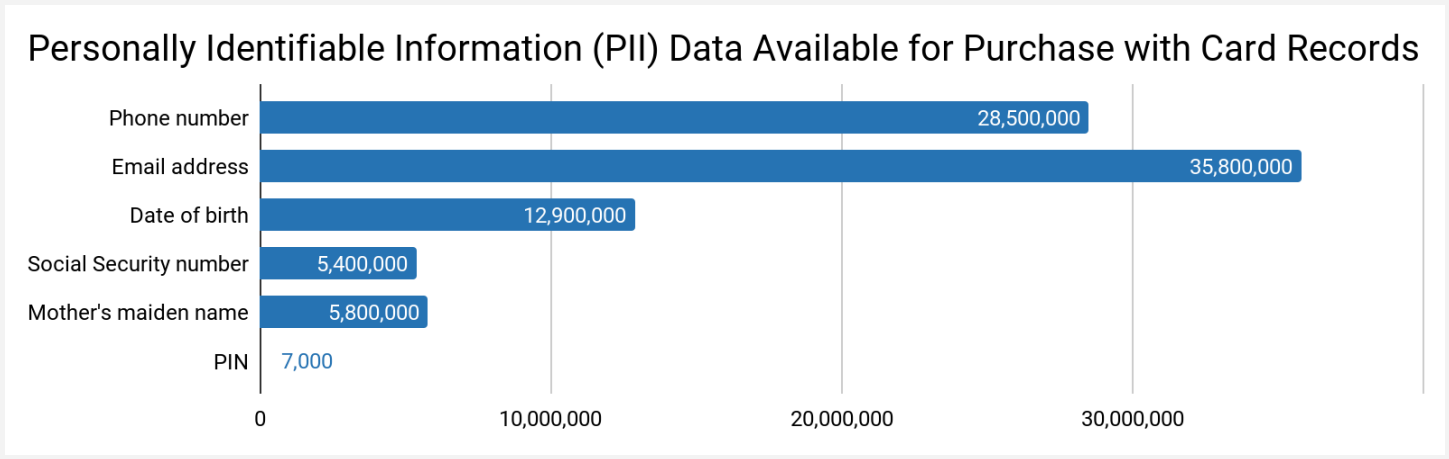


Figure 10: *In 2023, the amount of PII data available with for-sale card records predictably increased across the board (Source: Recorded Future)*

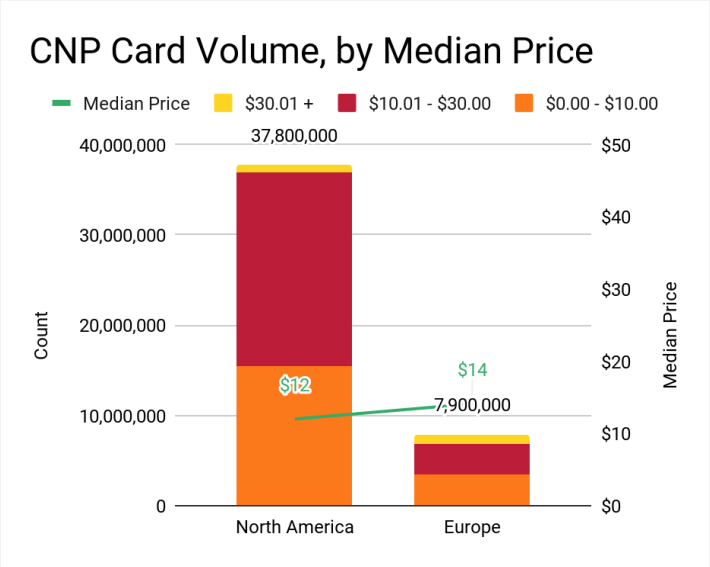
Carding Shop Metrics: 2023 Regional Highlights

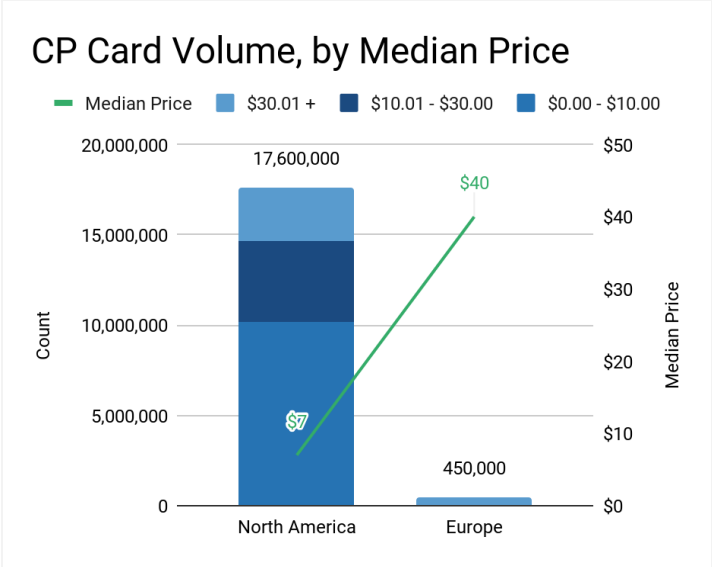
The supply of stolen payment cards in different regions of the world is always subject to variation, and this was no less true in 2023 than it will be in 2024. This discrepancy can exist across multiple geographies within a single card issuer's portfolio, and it is likely the result of various factors that either facilitate or complicate payment fraud with cards issued by FIs in certain countries, including:

- Stringent laws and regulations governing payments and transaction security, such as the European Union's second Payment Services Directive (PSD2)
- Widespread EMV chip deployment in certain regions of the world as opposed to others
- Cash economies or less robust e-commerce sectors within a region, which complicate payment card theft
- Lower average card spending limits in certain countries, which makes cards issued in those countries less appealing for international fraudsters

Ultimately, regional market differences likely signify that fraudsters perceive records in certain regions as having more or less value for fraud than those issued in other regions.

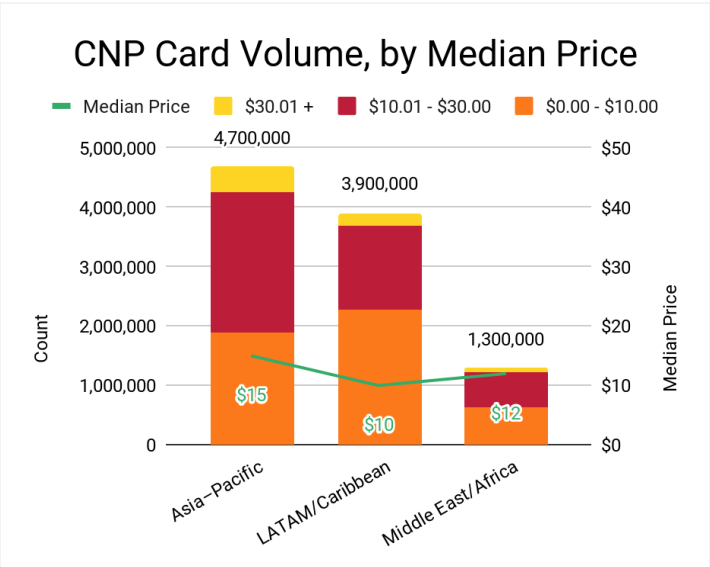
In 2023, while the supply of North American (NA) CNP and CP records exceeded European supply, the median price of European records was higher, suggesting a higher perceived potential return from fraud for European card records.

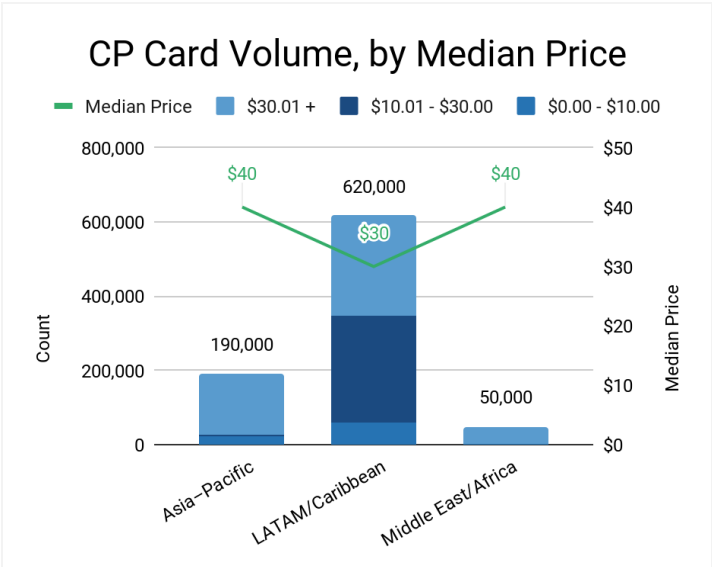




Figures 11 and 12: *The supply of NA CNP and CP card records outstripped that of European cards in 2023, but the higher prices of European cards suggest that fraudsters perceive they offer higher returns from fraud (Source: Recorded Future)*

Among other regions, the Asia–Pacific (APAC) region led in both the volume and median price of CNP records posted for sale on carding shops in 2023. CP trends were less revealing. In 2023, the sheer volume of Latin American and Caribbean (LATAM+C) CP records posted for sale was largely accounted for by a glut of 400,000 Brazilian CP records posted for sale throughout 2023.





Figures 13 and 14: *Outside of NA and Europe, APAC led in both card supply and median price on carding shops, and a glut of 400,000 Brazilian CP records in 2023 accounted for a surge in the supply of LATAM+C CP records (Source: Recorded Future)*

North America (NA)

Each year, North America (NA) — and in particular, the US — leads the world in total volumes of stolen cards posted for sale on carding shops. In 2023, the supply of US-issued records and Canada-issued records substantially increased. Among CP records, the US witnessed an increase in volumes posted, while Canada saw a minor decrease.

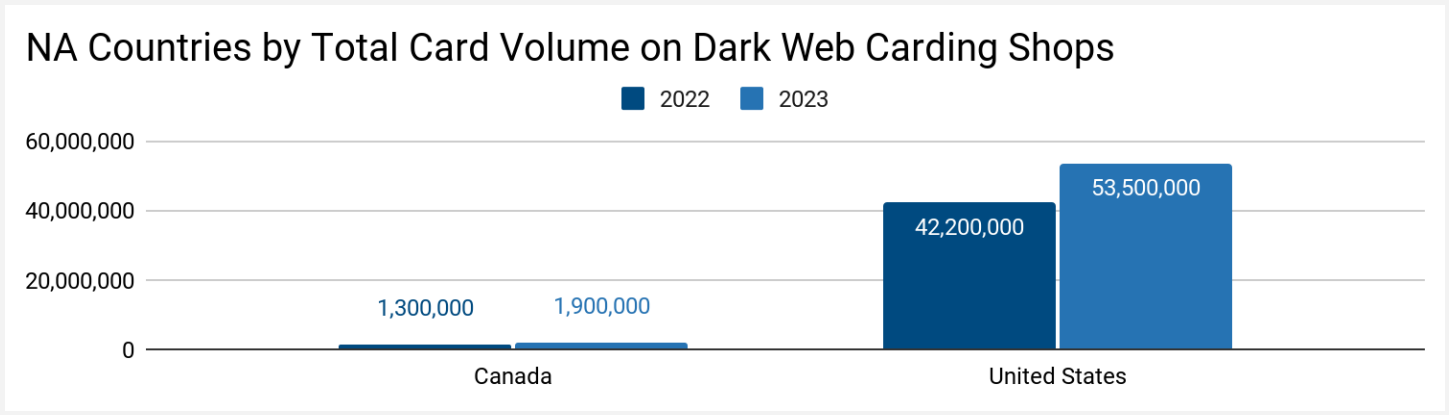
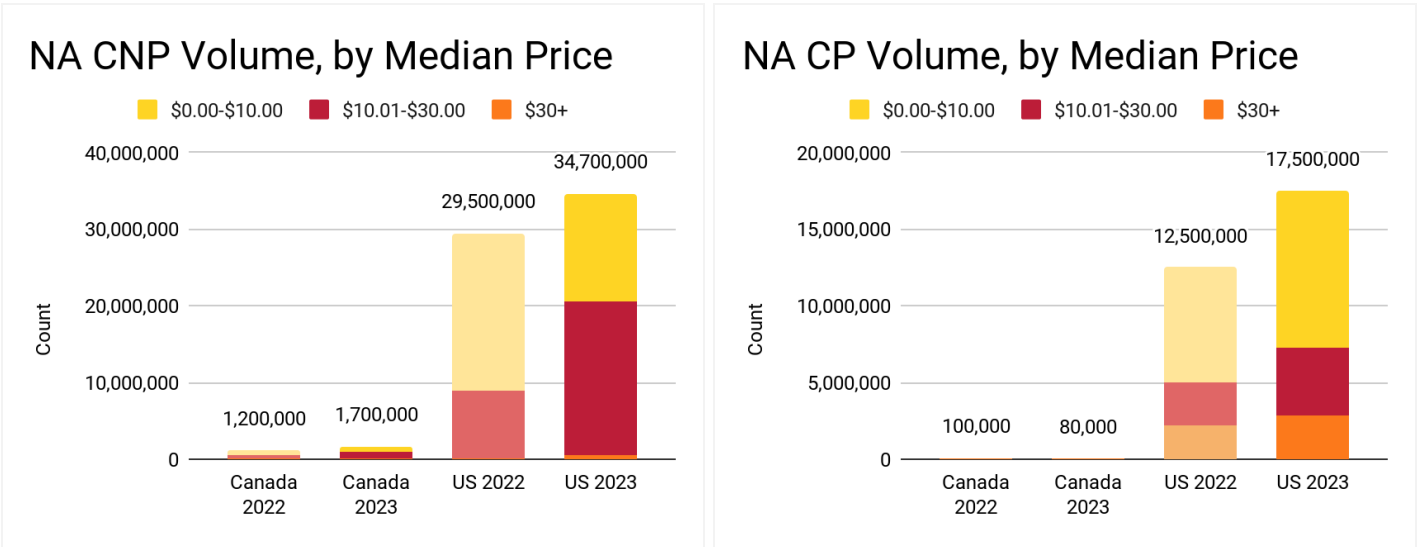


Figure 15: *2022 and 2023 volumes of both CNP and CP records posted to dark web carding shops for Canada and U.S. FIs (Source: Recorded Future)*

Precise comparisons between the prices of US- and Canada-issued records are nearly impossible due to the disparity in US and Canadian volumes. Nevertheless, we observed an increase in high- and medium-priced Canadian CNP records in 2023 as the share of low-priced Canadian CNP records dropped. For Canadian CP records, the share of both low- and medium-priced records fell. The share of high-priced Canadian CP records surged by 50 percentage points compared to 2022.



Figures 16 and 17*: As the total supply of NA CNP and CP records increased in 2023, the share of higher-priced records generally increased (Source: Recorded Future)*

Europe

In 2023, the UK, France, Spain, Türkiye, and Italy were the top 5 European countries by sheer volume of records posted for sale on dark web carding shops. The volume of Türkiye-issued records surged between 2022 and 2023, and growth in card volumes for the UK, France, and Spain occurred alongside parallel growth in Magecart e-skimmer infections targeting users from those countries. For these countries, only the volume of Italian card records decreased from 2022 to 2023.

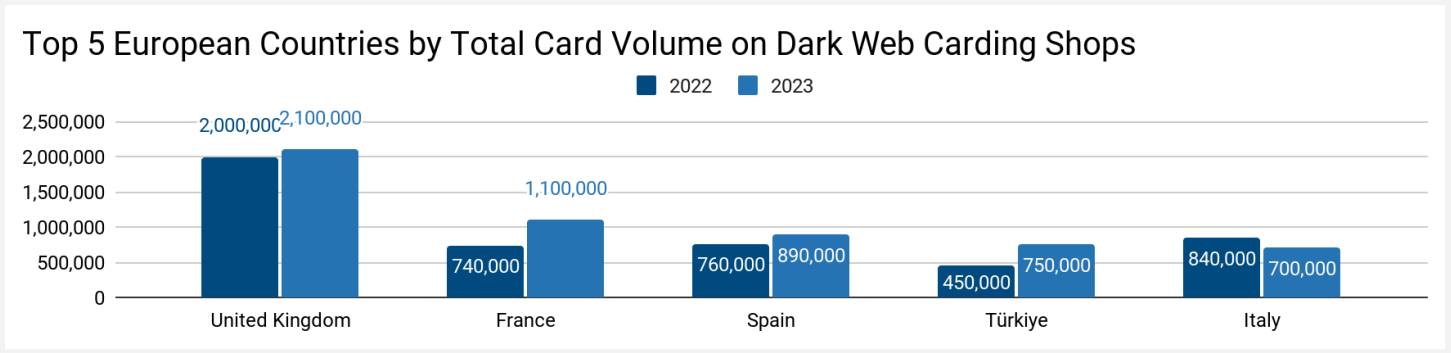


Figure 18: *As Türkiye-issued records nearly doubled between 2022 and 2023, increasing volumes for the UK, France, Spain, and Italy were accompanied by increasing Magecart infections targeting those countries' users (Source: Recorded Future)*

Latin America and the Caribbean (LATAM+C)

The top 5 LATAM+C countries by sheer volume of for-sale card records did not change from 2022 to 2023, though both Brazil and Mexico had lower record volumes in 2023. Volumes of cards issued by FIs in Peru, Argentina, and Columbia on carding shops in 2023, with Peru showing the highest percentage increase.

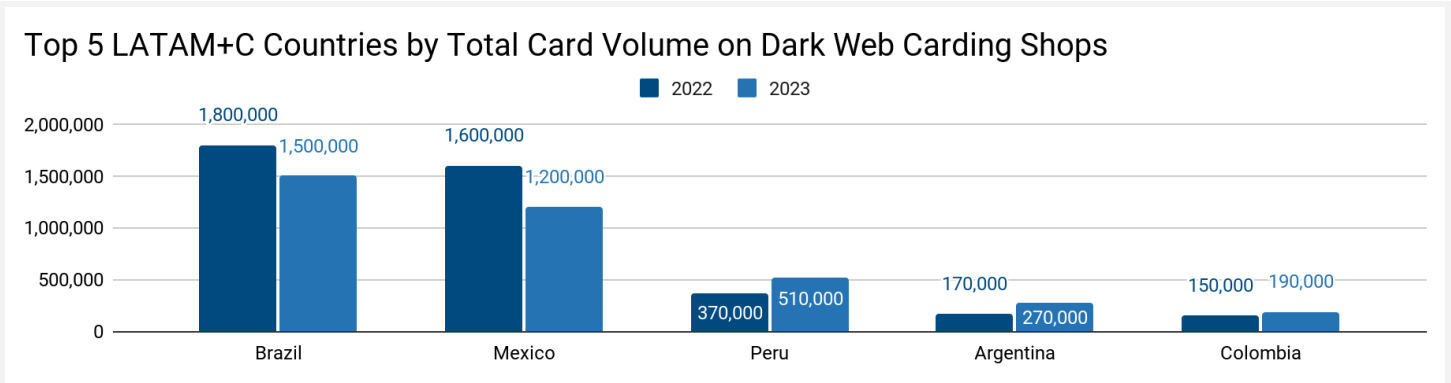


Figure 19: *Among the top 5 LATAM+C countries by sheer volume of cards posted for sale, Brazil's and Mexico's card volumes decreased year-on-year but remained the top 2 (Source: Recorded Future)*

Middle East and Africa (MEA)

Among the top 5 Middle Eastern and African (MEA) countries by sheer volume of records posted for sale in 2023, 3 countries had similar volumes compared to 2022. For the 2 outliers — South Africa and Egypt — the volume of cards issued from FIs in these countries respectively decreased and increased substantially compared to 2022.

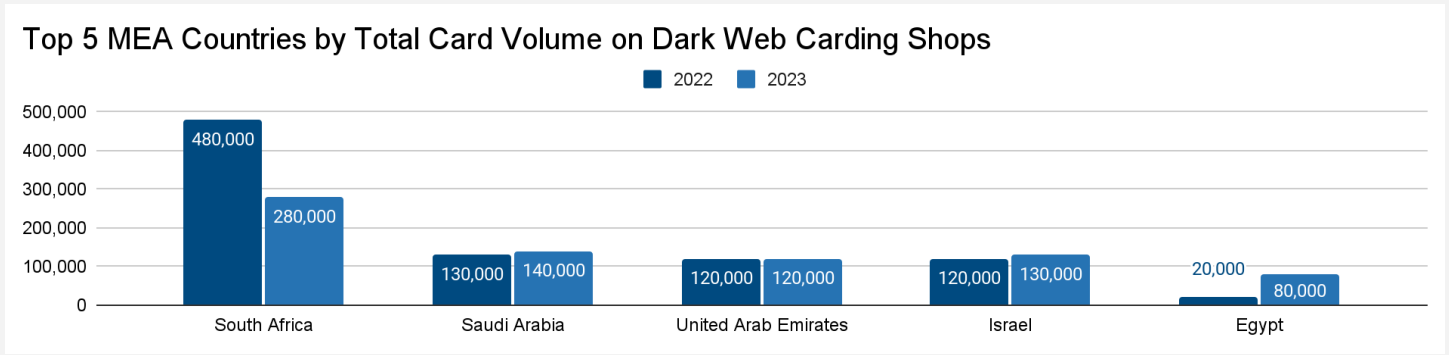


Figure 20: *In 2023, the volume of all cards posted for sale for 3 of the top 5 MEA countries by sheer volume was similar to 2022, with South Africa's and Egypt's card volumes substantially decreasing and increasing, respectively (Source: Recorded Future)*

Asia–Pacific (APAC)

Among the top 5 APAC countries by sheer volume of card records posted for sale in 2023, the volume of Japanese records increased most, likely as a result of records posted for sale on carding shops that predominantly offer Japanese records. This increase was accompanied by a surge in Magecart e-skimmer infections targeting Japanese users. At the same time, the volume of India-issued records posted for sale witnessed a net decrease. The supply of Indonesia-issued records experienced the highest percentage increase for the period.

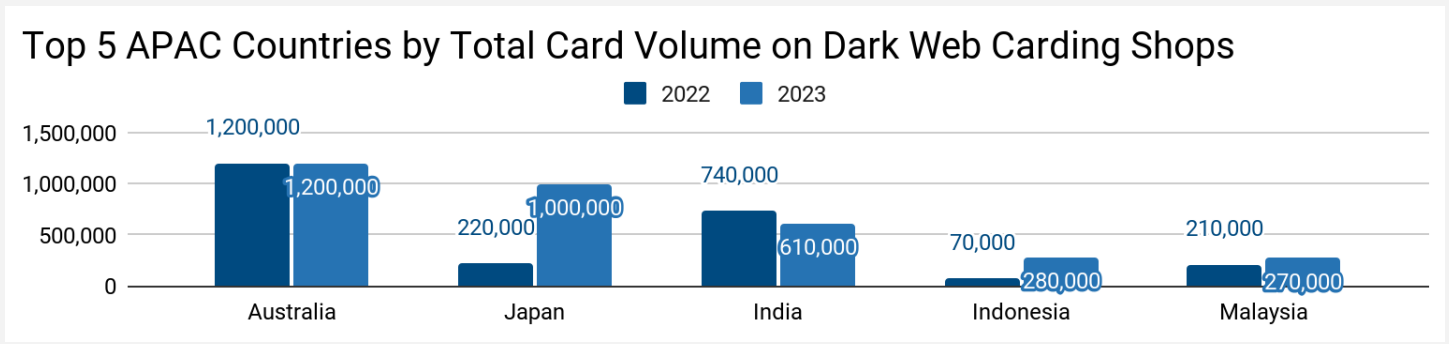


Figure 21: *Among the top 5 APAC countries by volume of cards posted for sale, Australia-issued card volumes remained stable as Japan- and Indonesia-issued card volumes surged and India-issued volumes decreased (Source: Recorded Future)*

Free Card Data: Telegram Sources Lead in Free Card Data Posted to All Dark Web and Clearnet Sources

In 2023, cybercrime-focused sources on Telegram were a rich source of free card data posted freely on the internet, demonstrating their growing importance. Despite vast increases in the volume of free card data on the dark web and other sources, free card data likely provided less value in potential fraud returns compared to for-sale data on carding shops. Altogether, threat actors posted 48 million full card records to various sources this year, up from 20.5 million in 2022. The vast majority of these records (41.3 million) were posted on Telegram sources, up nearly eightfold from 5.5 million in 2022. Fraudsters often use these Telegram sources to validate and/or generate payment card data.

The remaining free card data we analyzed in 2023 originated from carding shops (where free card data is often released to promote the source), pastebins, dark web forums, and other sources. Figure 22 below breaks down the most common sources for our free card data and includes roughly 94% of all free card data we analyzed from dark web and clearnet sources in 2023.

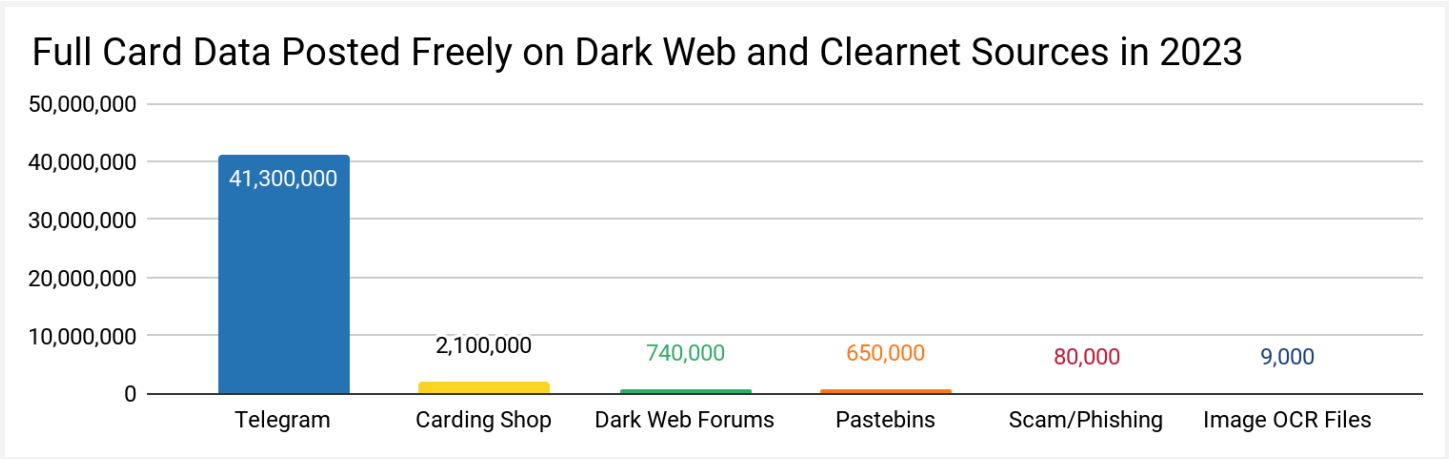
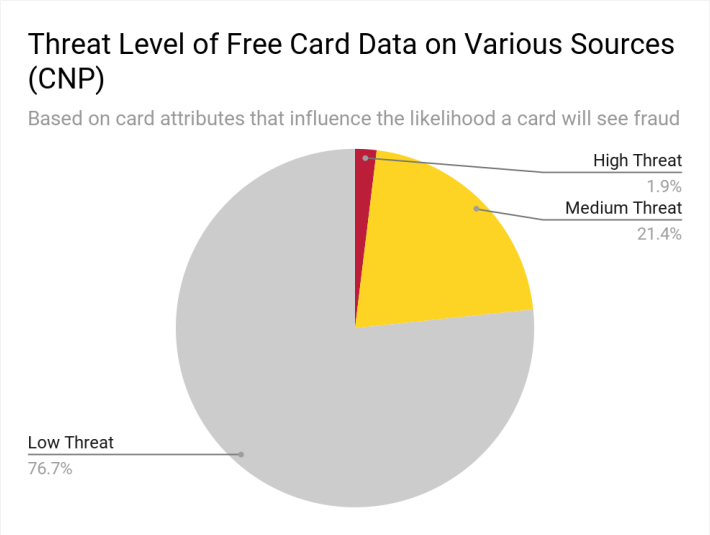
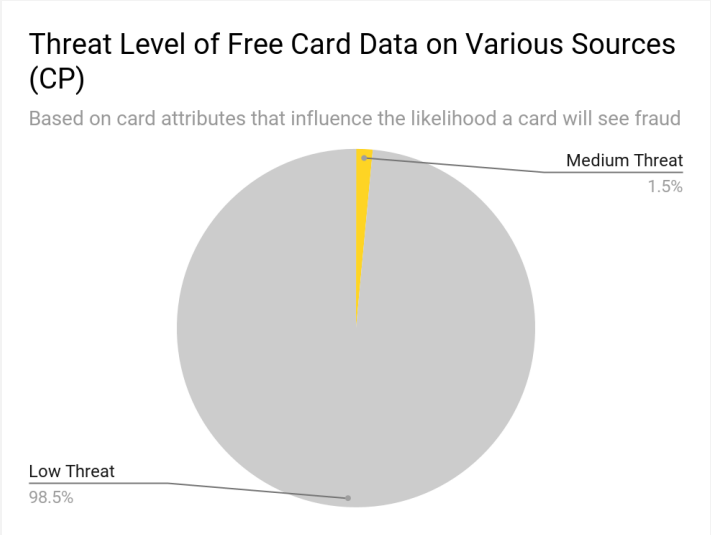


Figure 22: *In 2023, the vast majority of full card records originated from Telegram sources, indicating the growing relevance of Telegram sources for threat actors (Source: Recorded Future)*

Most free card records analyzed in 2023 belonged to low or medium threat segments, as is typical for free card records — a paradigm that is unlikely to change in 2024. High threat-level card segments are more likely to see fraud events; low threat-level card segments are less likely to see fraud events.





Figures 23 and 34: *In 2023, most full card records analyzed from the dark web and other sources belonged to low- or medium-threat segments, indicating they were less likely to see a fraud event (Source: Recorded Future Intelligence Cloud)*

As total volumes of free card data surged from 2022 to 2023, the proportion of free card numbers accompanied by card verification values (CVV, also known as card security codes, or CSC) and expiration dates also increased, most of which originated from Telegram sources. While these increases are likely an incidental result of our increased analysis of Telegram sources in 2023, it does demonstrate the growing value that Telegram sources offer fraudsters for card validation and generation.

Other cardholder data — including billing address, contact information, and highly sensitive PII, such as Social Security number (SSN), date of birth (DOB), or mother's maiden name (MMN) — also frequently accompanied free card records in 2023. Cybercriminals can use information accompanying low-validity, expired, or otherwise low-value payment card records to conduct spearphishing attacks and steal account login credentials before pivoting to targeted account takeover (ATO) attacks against victims' bank accounts.

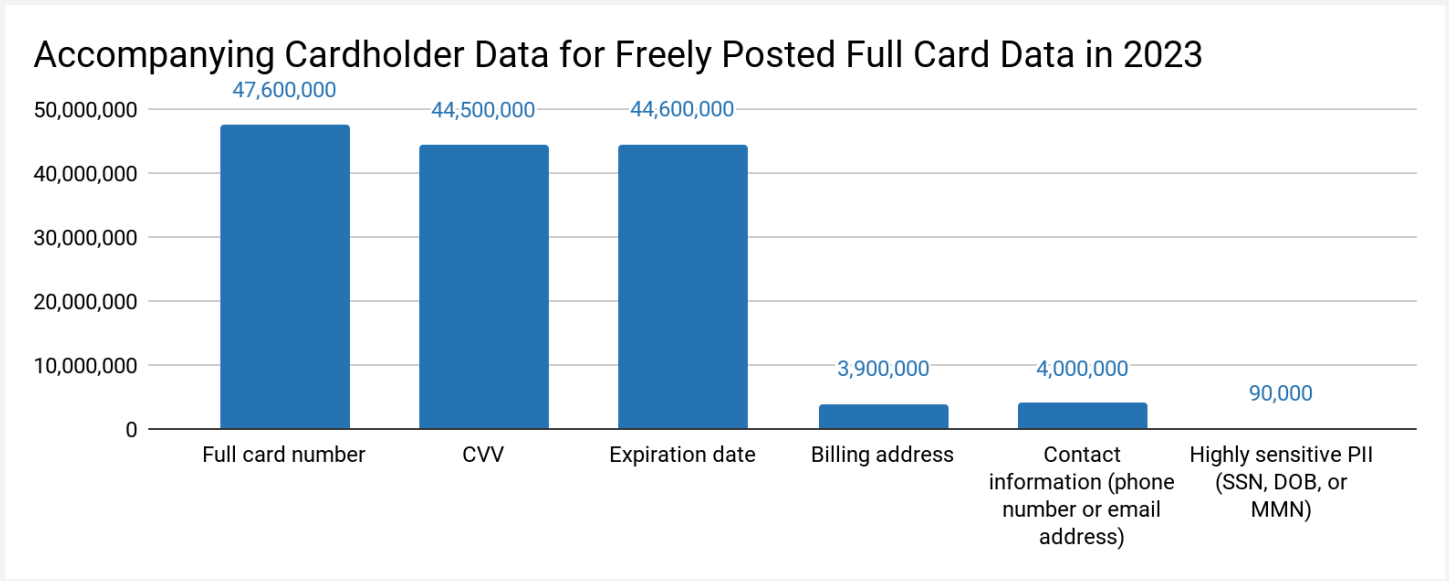


Figure 25: *In 2023, a higher proportion of free card data records was accompanied by CVV and expiration date, demonstrating the value Telegram sources offer fraudsters for card validation and generation (Source: Recorded Future)*

Tester Merchants: Despite Major Disruption, Dark Web Card-Testing Activity Keeps Calm and Carries On

Looking forward to 2024, card-testing activity is unlikely to go anywhere. Fraudsters conduct card-testing activity through low-value transactions and zero-dollar authorizations that frequently precede primary "cash-out" fraud events. Fraudsters likely access this card-testing functionality by various means, including:

- Fraudulent or compromised merchant account infrastructure under their control
- Dark web "checker" services that offer card-testing functionality to carding shops and threat actors through application programming interfaces (APIs), purpose-built websites, and Telegram bots
- Independent Telegram checker bots with similar card-testing services

In 2023, a joint law enforcement operation dismantled Try2Check, a major checker service that abused a major US-based payment processor's services for its card-testing functionality. However, while Try2Check's disruption may have diminished access for fraudsters accustomed to using its card-testing services, our analysis indicates that the quantity of tester accounts used by fraudsters slightly *increased* throughout 2023. This indicates that although Try2Check may have played a major role relative to other dark web checkers, it was ultimately part of an ecosystem, and fraudsters moved quickly to fill its vacuum.

In 2023, our analysis of 1,700 tester merchants surfaced various patterns in the MCCs and merchant acquirers most frequently associated with the checkers' tester merchants. Of the top 5 most common MCCs among tester merchants this year, only 8398 ("Organizations, Charitable and Social Service")

was dethroned from the Top 5 list of 2022. These MCCs and acquirers will likely remain common for tester merchants in 2024.

Top 5 Tester Merchant MCCs in 2023	Description
8011	Doctors–not elsewhere classified
5812	Eating Places and Restaurants
5999	Miscellaneous and Specialty Retail Stores
7299	Other Services–Not Elsewhere Classified
8099	Health Practitioners, Medical Services–Not Elsewhere Classified

Table 5: *In 2023, most tester merchants we surfaced were associated with the above MCCs (Source: Recorded Future)*

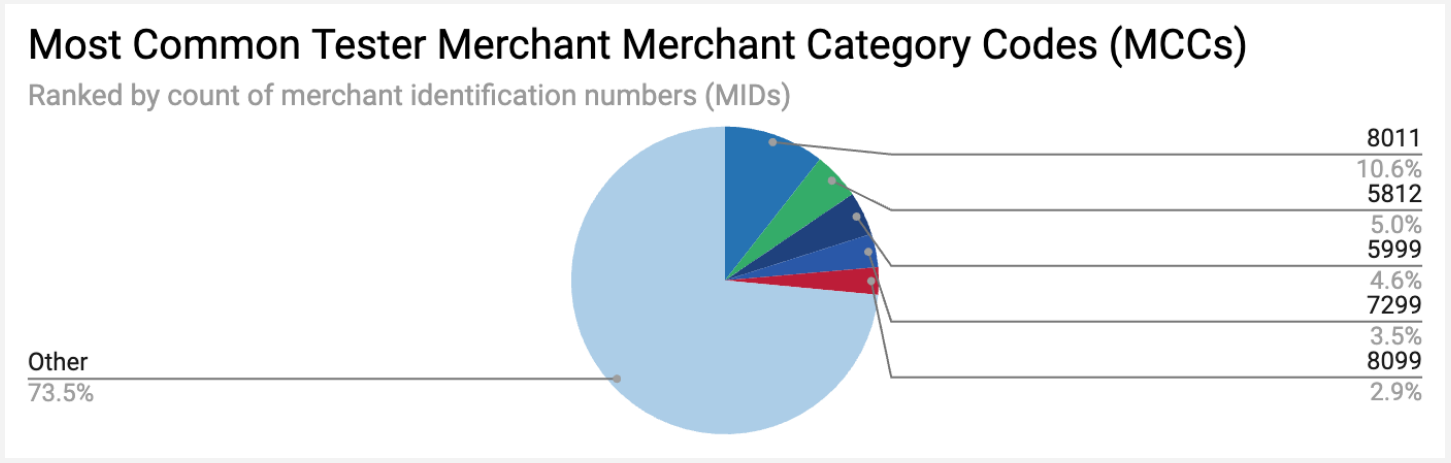


Figure 26: *In 2023, over a quarter of the tester merchant MIDs we surfaced used 1 of 5 MCCs (Source: Recorded Future)*

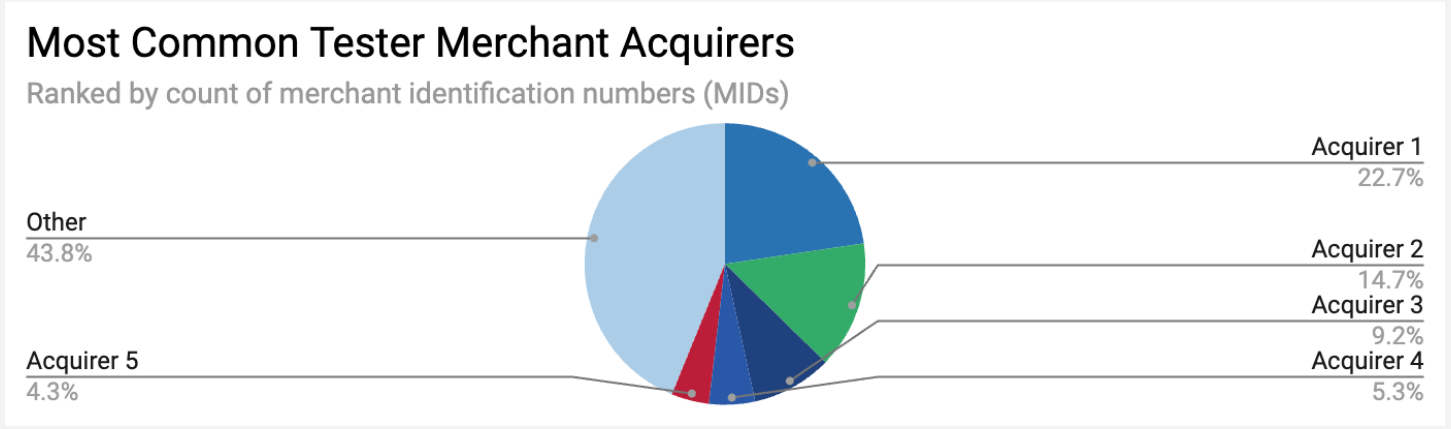


Figure 27: *In 2023, nearly 60% of the tester merchant MIDs we surfaced used 1 of 5 acquirers (Source: Recorded Future)*

Part of the reason we observe these patterns each year is that fraudsters can likely more readily exploit merchant accounts from certain acquirers or MCCs as tester merchants. The tester merchant accounts used by fraudsters generally fall into 1 of 2 categories:

- **Legitimate merchant accounts** that have been compromised or altered for card testing
- **Fraudulent merchant accounts** that have been created explicitly for card testing

In 2023, open-source research allowed us to determine 40% out of tester merchants we identified were likely to be fraudulent merchant accounts, whereas the remaining 60% were likely to be legitimate merchant accounts. Looking forward to 2024, fraudsters will likely continue to employ a mix of legitimate and fraudulent merchant accounts for their card-testing activity.

Fraudulent Transaction Placed: Fraudsters Use Sophisticated Tools, Nuanced Workflows, and Social Engineering Tactics to Slip Past Fraud Detection Rules

The make-or-break moment of any fraud scheme occurs with the final theft of a victim's money or data. In 2023, we observed 2 key themes in fraudsters' efforts to effect cash-out and data theft attempts, both of which are likely to continue playing out in 2024:

- Growing sophistication of technical solutions combined with increasingly nuanced workflows
- Growing reliance on social engineering tactics, particularly for scam pages and phishing lures

Sophisticated Technical Solutions Combined with Increasingly Nuanced Workflows

Our analysis in 2023 surfaced various advanced fraud schemes that depended on sophisticated technical solutions, tailored services, nuanced workflows, or AI to bypass fraud detection programs.

- **Workflows and technical solutions for 3DS bypass are gaining popularity on cybercriminal sources.** From September 2022 to May 2023, the threat actor "vikis", operating under the alias "morettis", advertised various versions of the 3DS-bypass software "VBV Bypass" on multiple dark web forums. According to morettis, the software can be used to bypass 3DS authentication for transactions conducted with a growing number of merchants and payment processing services worldwide, as well as over 7,000 payment card BINs from over 200 card issuers, including 80 US and Canadian FIs. Our analysis indicated the software was effective when used as advertised.

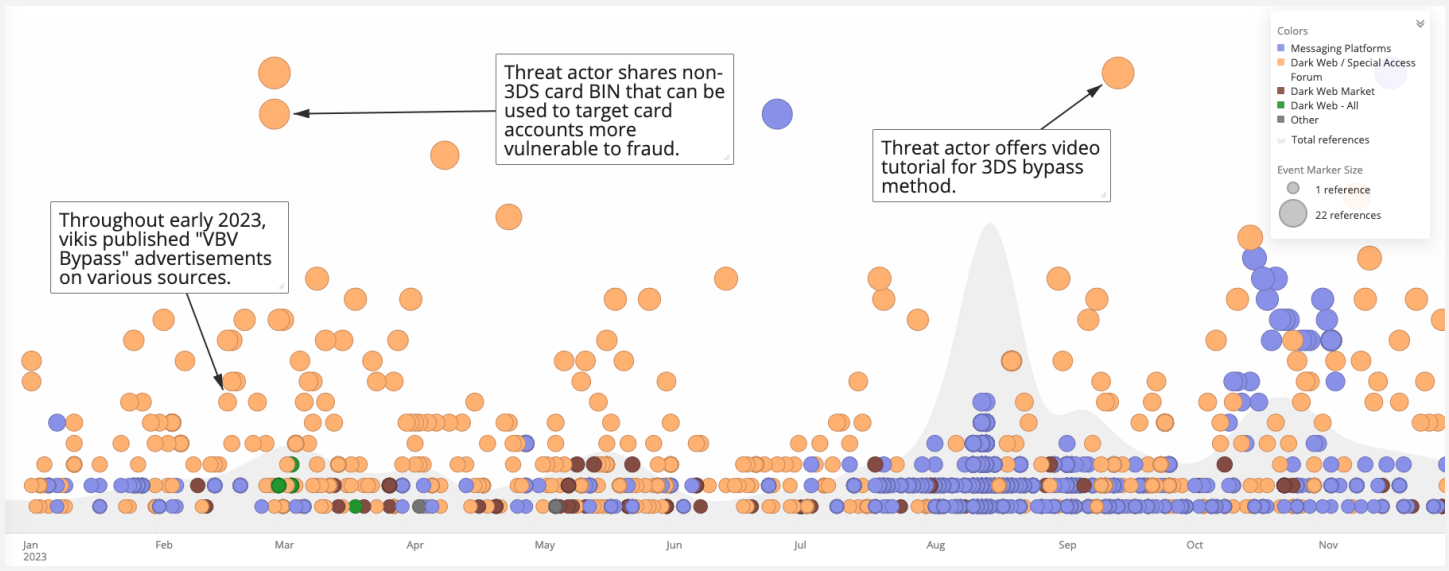


Figure 28: *In 2023, the frequency of references to 3DS bypass on various sources increased by nearly 20% compared to 2022 (Source: Recorded Future Intelligence Cloud)*

- **Increasingly sophisticated schemes allow threat actors to compromise and monetize financial data as part of an integrated fraud-based malvertising ecosystem.** In February 2023, Spamhaus reported a surge in malvertising activity that exploited a popular advertising platform, which was accompanied by a massive increase in references to an online advertising platform on various sources. Our analysis subsequently confirmed that threat actors routinely offer malvertising-as-a-service on the dark web by linking stolen payment cards or other payment methods to compromised or fraudulent ad accounts. Using funds from these stolen payment methods, fraudsters create illicit "malvertising agencies" that purchase legitimate ad inventory for malvertising attacks. In turn, these attacks distribute scam pages, phishing pages, and stealer malware that can compromise additional advertising accounts and payment methods, indirectly creating a vicious cycle.

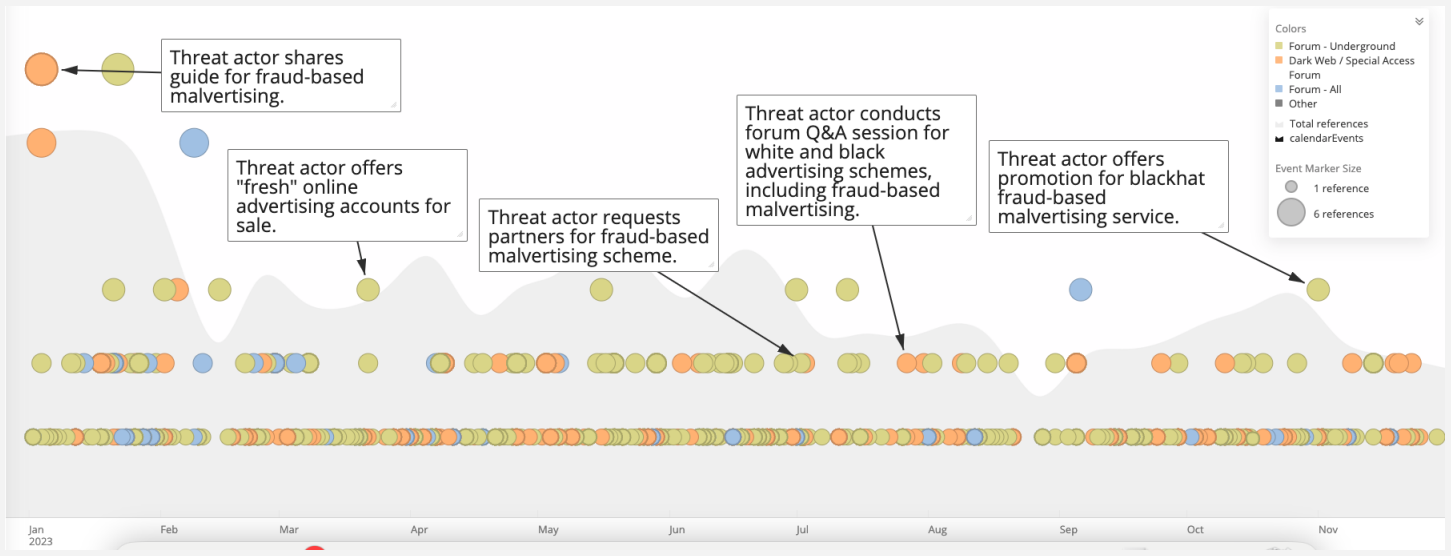


Figure 29: *In 2023, dark web, underground, and clearnet forum references to an online advertising platform grew by 17% compared to 2022; many of these references were related to a fraud-based malvertising ecosystem (Source: Recorded Future Intelligence Cloud)*

- **Information sharing, particularly through detailed guides on cybercriminal sources, facilitated NAF in 2023.** For example, in March 2023, the Ukrainian company Vektor T13 Technologies LLC released the course "Ethical hacking of antifraud system" in collaboration with another firm. In this course, a lecturer from Vektor T13 taught attendees the skills necessary to bypass anti-fraud technologies. Vektor T13 is a provider of various software products and analytical services that threat actors can likely use to assist in bypassing anti-fraud systems to conduct online fraud, including NAF. Threat actors continued to reference Vektor T13 on various cybercrime-focused sources throughout 2023.

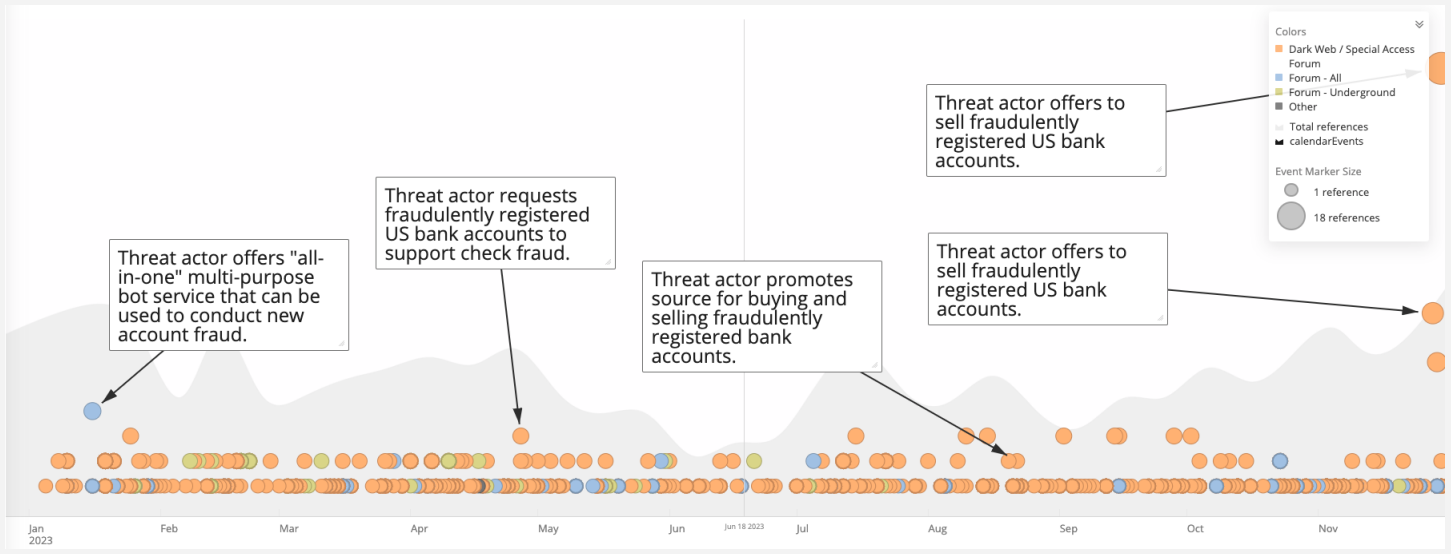


Figure 30: *In 2023, dark web, underground, and clearnet forum references to new account fraud — including for tutorials, sales offers, and purchase offers — increased by over 60% compared to 2022 (Source: Recorded Future Intelligence Cloud)*

- **Cybercriminals seized upon Telegram to enable their fraud schemes.** Our analysis indicated a flourishing cybercrime community has developed on Telegram channels to support check fraud, with at least 100,000 check images published to Telegram in 2023, and revealed that cybercriminals develop sophisticated cyber-based methods to cash out fraudulent checks. Additionally, throughout the year, fraudsters demonstrated reliance on free Telegram checker bots. These sources have card-testing functionality similar to that of dark web checker services and can support account enumeration attacks. Account enumeration attacks occur when fraudsters generate and validate card data for fraud.

Telegram Source Type	Count of Channels
All sources	398
Sources with free card validation capabilities	**304**
Sources with free card generation capabilities	**172**

Table 6: *Of the Telegram sources we analyze, most offer fraudsters free card validation and/or generation services (Source: Recorded Future)*

- **Cybercriminals developed and employed AI-based workflows to facilitate fraud and cybercrime schemes, particularly with voice cloning technology.** In February 2023, VICE reporter Joseph Cox claimed he had successfully passed his bank's voice authentication system using an AI-generated voice-cloning sample, a tactic fraudsters later employed successfully to siphon $243,000 from the account of the CEO of a UK-based energy firm. Meanwhile, in March 2023, the FTC reported that scammers had begun to use AI to enhance their family emergency scams. Additionally, as part of Vektor T13's anti-fraud system bypass course referenced above, the course lecturer demonstrated how to use generative AI to analyze web page source code in order to assess the strengths and weaknesses of websites' anti-fraud systems.

Social Engineering Tactics

As cybercriminals applied sophisticated technical solutions to bypass fraud detection rules, they also demonstrated increased reliance on social engineering tactics that manipulate victims into facilitating the theft, exploiting the unwitting assistance of victims to bypass banks' fraud-detection mechanisms entirely. This trend was almost certainly facilitated by the 2023 advent of accessible generative AI and will likely continue into 2024.

Fraudsters' social engineering efforts were most apparent in their scam and phishing website campaigns, a trending threat in 2023. These scam and phishing campaigns combined cookie-cutter designs and open-source tools with sophisticated technical means to disseminate their scams, cash out victims' payment cards and crypto wallets, and steal victim data. Scam operators typically demonstrate a superb understanding of consumer psychology to maximize the impact of their social engineering tactics and scam campaigns, and third-party dark web services allow threat actors to outsource the creation or operation of their scam and phishing campaigns.

Examples of these services include:

- Holistic third-party “fraud-as-a-service” offerings that offer all-in-one scam/phishing services
- Design services for scam ads, websites, and landing pages to create appealing scam lures
- SMS spam/smishing services and web traffic services that drive victims to scam pages

Mitigations

Increase coordination between CTI and fraud teams as part of a fraud fusion effort to reduce the threat posed by the convergence of cyber and fraud threats. Fraudsters' increasing sophistication and reliance on social engineering are likely part of a two-pronged, cyber-based assault against the rigorous fraud detection rules employed by FIs, and the potency of this combination is grounded in the fact that most FIs establish distinct business units with separate practices to mitigate cyber and fraud risk. In particular, increasing resource-sharing between CTI and fraud teams will likely improve business outcomes while reducing operating costs through shared resources, and the concerted development of specific use cases for coordination between CTI and fraud units will provide a foundation for more effective future cooperation. Possible use cases for CTI and fraud teams include the following:

New Account Fraud (NAF) and Account Takeover (ATO) Attacks

1. Coordinate to identify patterns in user activity, network information, system information, and hardware parameters for card or bank accounts that eventually see fraud events. Take note of inconsistent identifiers that suggest the user masked their activity with anti-detection browsers or proxy services.
2. Using these patterns, build a fraud detection query to surface additional accounts likely to be fraudulent.
3. Raise the threat level for user activity, transactions, and financial transfers to and from these accounts.
4. Leverage reanalysis to refine your query and continue surfacing accounts as part of an intelligence cycle.

Take Preemptive Action on Dark Web Intelligence Reporting

- Leverage dark web intelligence reporting — particularly cybercrime tutorials that offer a "fraudster's-eye view" of fraud schemes — to identify and mitigate workflows fraudsters consider effective. To do this, use the analytical process described above.
- Leverage dark web intelligence reporting to identify whether fraudsters target your organization, card BIN segments, and merchants. Take appropriate action, such as by raising the threat level for cards that transact with identified cash-out merchants.

Conduct Analysis of Suspected CPPs and Tester Merchants

- For suspected CPPs, use technical analysis to confirm sources of compromise by searching for Magecart e-skimmer infection IOCs. For card accounts that have experienced fraud events, conduct transaction analysis to identify potential card-testing activity.
- Leverage reanalysis to identify similar e-skimmer infection IOCs or card-testing activity across a wider sample of merchants and card accounts, respectively, that may pose a threat to your portfolio.
- Raise the threat level for all card accounts that transact with confirmed CPPs or tester merchants until the breach or card-testing activity is remediated.

Outlook

Keeping in mind our observations from 2023, 2 trends will likely influence the payment fraud threat landscape in 2024.

First, fraudsters participating in the dark web payment fraud underground will almost certainly continue to persevere, refining their methods as they continue to find ways around the barriers FIs put up to protect their customers. FIs can reduce the threat posed by this trend through tactical measures, such as operationalizing Recorded Future's card and merchant datasets. While we cannot predict with certainty the specifics of how stolen card supply or demand on carding shops will look, they will likely continue to serve as a major source of stolen card data regardless of what the year throws at them. Similarly, although specific Magecart e-skimmer deployment or data exfiltration techniques may evolve, the attack vector will likely remain viable in 2024. Checkers will continue to offer card-testing services to fraudsters and other dark web entities through tester merchants, and Telegram sources will continue to serve as viable tools for fraudsters seeking to generate or validate card data. While we cannot accurately predict a full recovery or resurgence to pre-2022 levels, fraudsters' adaptability and resilience in the face of 2022's system shocks and the 2023 aftermath demonstrate that payment fraud is not going anywhere.

Second, fraudsters' growing reliance on cyber-based fraud schemes and social engineering will continue to empower them to bypass rules-based fraud detection systems. Because this combination of strategies exploits the limitations of rules-based systems more generally, FIs can reduce the threat posed by this trend on a strategic level by increasing coordination efforts between their CTI and fraud business units. Note that this convergence of cyber and fraud risk domains was not a novel development in 2023 but rather part of a continuing trend that is likely to become even more prominent in 2024. In this respect, the advent of viable generative AI tools in early 2023 is unlikely to significantly alter the balance between fraudsters and the organizations that seek to stop them, even as it changes the surface of the threat landscape. In 2024, AI will likely become yet another front in the arms race between fraudsters seeking methods to bypass fraud controls effectively and the organizations that erect those fraud controls to stop them.

Recorded Future®

About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for clients, enables tangible outcomes, and prevents business disruption.

About Recorded Future®

Recorded Future is the world's largest threat intelligence company. Recorded Future's Intelligence Cloud provides end-to-end intelligence across adversaries, infrastructure, and targets. Indexing the internet across the open web, dark web, and technical sources, Recorded Future provides real-time visibility into an expanding attack surface and threat landscape, empowering clients to act with speed and confidence to reduce risk and securely drive business forward. Headquartered in Boston with offices and employees around the world, Recorded Future works with over 1,700 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com