CYBER THREAT ANALYSIS

Recorded Future®

Payment Fraud Intelligence

January 21, 2025

Annual Payment Fraud Intelligence Report: 2024

The volume of stolen data surged in 2024. Threat actors posted 269 million stolen cards and 1.9 million checks for sale or freely, and we found more new e-skimmer infections stealing card data than ever before.

Threat actors are increasingly using digital wallets for fraud. They leverage security mechanisms as fraud mechanisms — and social engineering and one-time password intercept help them do it.

In the USA, check fraud is here to stay. Even so, new improvements in fraud intelligence and a realignment in business priorities can help financial institutions combat check fraud better than ever before.

Executive Summary

Evolution characterized the fraud threat landscape in 2024, promising challenges for 2025. Analysis of Recorded Future® Payment Fraud Intelligence data indicated the surging availability of stolen data: 269 million card records were posted on dark web and clear web sources alongside 1.9 million stolen US bank checks dated from 2024. Meanwhile, our merchant datasets revealed increasing volumes of scam merchant accounts meant for fraud, Magecart e-skimmer infections stealing data from legitimate e-commerce websites, and "tester" merchants abused for fraudulent card validation activity. Most troubling, our observations on dark web sources indicated a broad appetite among threat actors to embrace and exploit the weaknesses of modern payment security technologies — or even leverage them for fraud. This finding was supported by our analysis of numerous fraud workflows, scam operations, and e-skimmer groups. These factors likely indicate a shift among threat actors toward abuse of the trust systems and technologies that prevent fraud in order to commit fraud, allowing them to embrace security mechanisms as fraud mechanisms. To a large extent, artificial intelligence (AI) enablement and refined social engineering tactics are helping threat actors make this shift.

These trends and more raised financial fraud risks for financial institutions, merchants, payment service providers, and others in the e-commerce and banking industries. Mitigations that will likely reduce these risks broadly come in two flavors: first, increasing the rigor of customer onboarding and verification processes, and second, incorporating fusion intelligence deliverable-feedback loops that harmonize cybersecurity and anti-fraud assets to prevent fraud more effectively. We detail specific strategies to achieve these outcomes in the Mitigations section of this report.

Looking forward, we make three major predictions for 2025:

- Digital e-skimming and scam e-commerce will drive data compromise events in 2025, especially as fraudsters prioritize digital wallets for cash-out schemes.
- Dark web marketplaces will continue to serve as a centerpiece of the payment fraud ecosystem, with Telegram and similar platforms reserved for less experienced threat actors.
- The explosion in check fraud seen in the United States over the past three years will not abate, but improving check fraud prevention methods will equip financial institutions to reduce check fraud losses more effectively.

Key Findings

- **Magecart e-skimmers remained highly viable for data theft.** In 2024, three primary factors defined the Magecart threat landscape: soaring infection volume following the discovery of CVE-2024-34102 ("CosmicSting"), e-skimmer kits that lower technical barriers for threat actors, and the continuing development of Magecart tactics, techniques, and procedures (TTPs). Altogether, the volume of unique e-commerce domains infected by e-skimmers increased by nearly threefold from last year.
- **Scam e-commerce websites became an increasingly salient threat in 2024.** This year we identified nearly 1,200 scam website domains linked to networks of scam merchant accounts. Most scam merchant accounts we discovered were registered in the United Kingdom and Hong Kong, and scam TTPs grew more subtle and sophisticated throughout the year.
- **Trends in identified common points of purchase (CPPs) indicated an evolving threat landscape.** Restaurants remained preeminent among breach sources, and our research continued to highlight the outsize impact that platform breaches have on the e-commerce industry. At the same time, breaches at fashion stores became increasingly common, a trend largely driven by the increasing volume of scam websites.
- **Spikes in the volume of stolen card data on dark web sources broadly indicated increased availability of stolen card and cardholder data.** Threat actors posted 70 million more card records for sale in 2024 compared to 2023. Deeper implications for the year's surge in for-sale stolen data remain unclear, but the increase likely reflected both more frequent reposting and data compromise events. Card-not-present (CNP) data continued to dominate among card data, even as effective card-present (CP) fraud workflows persisted.
- **Telegram continued to remain in play as a source of unique free card data.** The volume of non-unique card data on Telegram dropped in the wake of Pavel Durov's arrest, but Telegram remained a reliable source of unique data, suggesting threat actors will likely continue operating on the platform.
- **Dark web card validation activity increased in 2024, and merchant category trends reflected likely access methods threat actors used to abuse tester merchants.** We observed more dark web checker services than in preceding years. A third of all tester merchants belonged to one of five merchant categories, which likely reflected the access methods threat actors used to abuse the merchants for testing activity. Generally, checkers preferred to abuse tester merchants over short-term, non-consecutive periods, likely to avoid detection.
- **Rampant reposting and geographic trends defined the check fraud threat landscape.** 1.9 million stolen US bank checks were posted for sale on Telegram sources, but nine out of ten of them were reposted. We attributed a disproportionate volume of stolen checks to the US East Coast, and threat actors reposted checks from payers in certain states more frequently than others, suggesting heightened threat actor demand may exist for stolen checks in those states.
- **Growing sophistication and an appetite to embrace the opportunities and limitations of anti-fraud technologies and processes defined the dark web fraud landscape in 2024.** Threat actor discourse pointed to workflows abusing security-focused financial technology, nuanced verification bypass, and a steady reliance on complex money laundering services and tactics.

Table of Contents

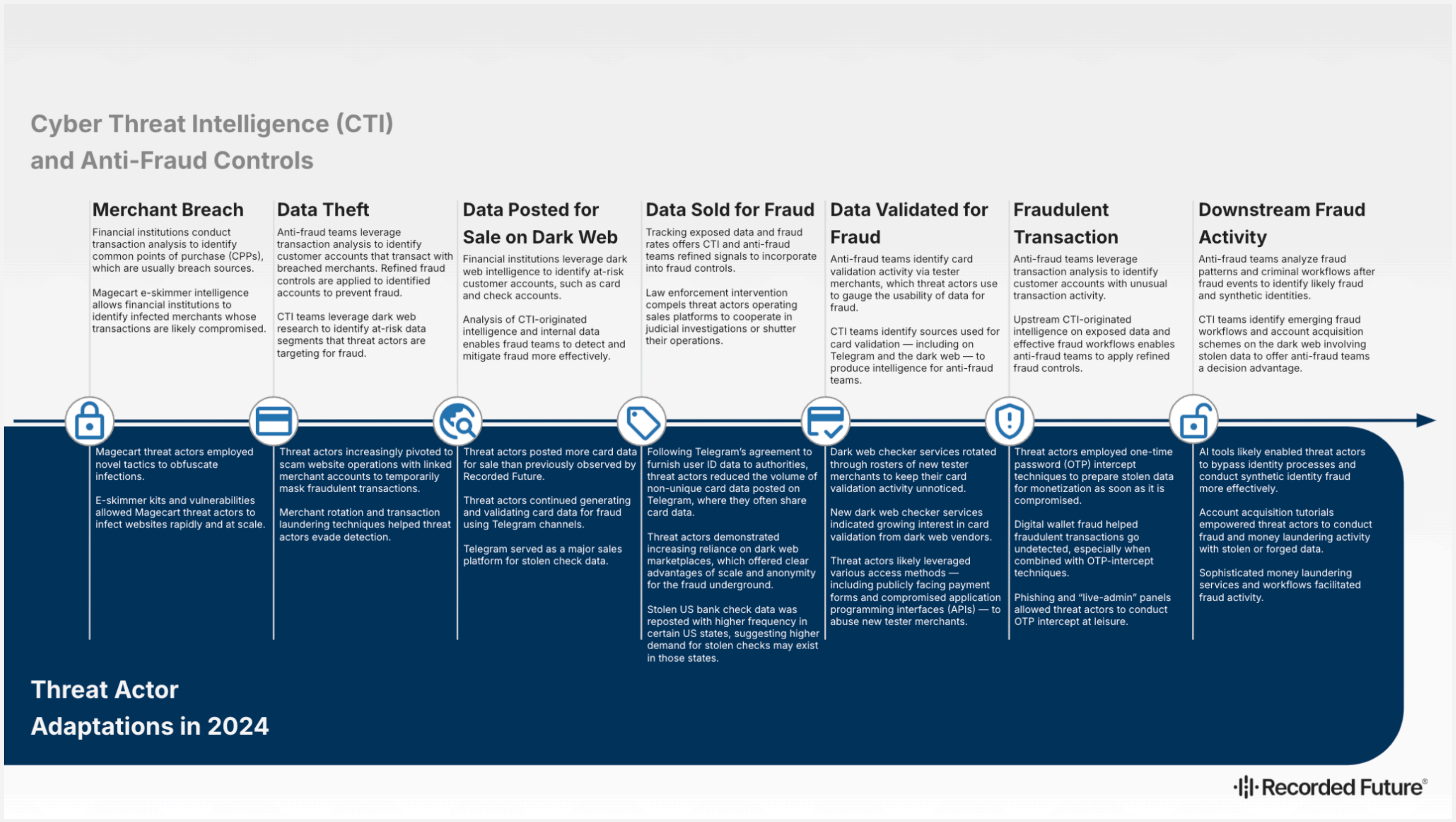
Threat Analysis

For financial institutions, fraud is tricky. We dub this challenge the Castle Dilemma. Cyber threat intelligence (CTI) teams and their partner cybersecurity assets are superbly equipped to protect their institution — the castle — from direct attacks, but CTI teams encounter challenges enabling anti-fraud teams to protect customers. To surmount the Castle Dilemma, CTI teams and anti-fraud teams must employ an orderly intelligence-feedback loop and enjoy support from leadership to prevent fraud effectively, protect their customers, and protect their organization's reputation.

Recent years have seen financial institutions engage in greater CTI–fraud fusion efforts to overcome the Castle Dilemma and enable more effective anti-fraud action. In 2024, the selective pressures of these successful fusion efforts became most evident in fraudsters' increasing sophistication and productivity. Throughout the year, many tried-and-true fraud TTPs likely remained effective, as indicated by customer feedback and our threat research, which we describe in this report. At the same time, two clear new patterns emerged, painting a picture of what is likely to come for the fraud threat landscape in 2025:

- **Threat actors enthusiastically and effectively abused the trust systems emplaced by merchants and financial institutions to increase customer convenience and security.** Threat activity pointed toward increasing appetite to transform anti-fraud mechanisms into fraud mechanisms, turning the Castle Dilemma on its head.
- **Threat actors are fluidly leveraging social engineering to fill in the gaps for technical, cyber-enabled fraud attack chains.** In many ways, this is a return to form for the fraud threat landscape and represents what might be considered a dark-side fusion: just as upstream CTI can empower anti-fraud teams to tackle modern fraud challenges, social engineering can bridge weaknesses in fraud attack chains, minimizing their disruption points.

In this report, we profile the evolving fraud threat landscape for 2024 to better understand what is to come in 2025. This report's research is grounded in analysis of our product datasets, which enable financial institutions, card networks, payment service providers, merchants, and other entities in the banking and e-commerce industries to proactively detect and prevent fraud with timely and actionable upstream intelligence. Our research also incorporates open-source information and an analysis of threat actor discourse on dark web sources. All research in this report was current as of January 6, 2024.



Cyber Threat Intelligence (CTI) and Anti-Fraud Controls

Merchant Breach

Financial institutions conduct transaction analysis to identify common points of purchase (CPPs), which are usually breach sources.

Magecart e-skimmer intelligence allows financial institutions to identify infected merchants whose transactions are likely compromised.

Data Theft

Anti-fraud teams leverage transaction analysis to identify customer accounts that transact with breached merchants. Refined fraud controls are applied to identified accounts to prevent fraud.

CTI teams leverage dark web research to identify at-risk data segments that threat actors are targeting for fraud.

Data Posted for Sale on Dark Web

Financial institutions leverage dark web intelligence to identify at-risk customer accounts, such as card and check accounts.

Analysis of CTI-originated intelligence and internal data enables fraud teams to detect and mitigate fraud more effectively.

Data Sold for Fraud

Tracking exposed data and fraud rates offers CTI and anti-fraud teams refined signals to incorporate into fraud controls.

Law enforcement intervention compels threat actors operating sales platforms to cooperate in judicial investigations or shutter their operations.

Data Validated for Fraud

Anti-fraud teams identify card validation activity via tester merchants, which threat actors use to gauge the usability of data for fraud.

CTI teams identify sources used for card validation — including on Telegram and the dark web — to produce intelligence for anti-fraud teams.

Fraudulent Transaction

Anti-fraud teams leverage transaction analysis to identify customer accounts with unusual transaction activity.

Upstream CTI-originated intelligence on exposed data and effective fraud workflows enables anti-fraud teams to apply refined fraud controls.

Downstream Fraud Activity

Anti-fraud teams analyze fraud patterns and criminal workflows after fraud events to identify likely fraud and synthetic identities.

CTI teams identify emerging fraud workflows and account acquisition schemes on the dark web involving stolen data to offer anti-fraud teams a decision advantage.

Threat Actor Adaptations in 2024

Merchant Breach:

Magecart threat actors employed novel tactics to obfuscate infections.

E-skimmer kits and vulnerabilities allowed Magecart threat actors to infect websites rapidly and at scale.

Data Theft:

Threat actors increasingly pivoted to scam website operations with linked merchant accounts to temporarily mask fraudulent transactions.

Merchant rotation and transaction laundering techniques helped threat actors evade detection.

Data Posted for Sale on Dark Web:

Threat actors posted more card data for sale than previously observed by Recorded Future.

Threat actors continued generating and validating card data for fraud using Telegram channels.

Telegram served as a major sales platform for stolen check data.

Data Sold for Fraud:

Following Telegram's agreement to furnish user ID data to authorities, threat actors reduced the volume of non-unique card data posted on Telegram, where they often share card data.

Threat actors demonstrated increasing reliance on dark web marketplaces, which offered clear advantages of scale and anonymity for the fraud underground.

Stolen US bank check data was reposted with higher frequency in certain US states, suggesting higher demand for stolen checks may exist in those states.

Data Validated for Fraud:

Dark web checker services rotated through rosters of new tester merchants to keep their card validation activity unnoticed.

New dark web checker services indicated growing interest in card validation from dark web vendors.

Threat actors likely leveraged various access methods — including publicly facing payment forms and compromised application programming interfaces (APIs) — to abuse new tester merchants.

Fraudulent Transaction:

Threat actors employed one-time password (OTP) intercept techniques to prepare stolen data for monetization as soon as it is compromised.

Digital wallet fraud helped fraudulent transactions go undetected, especially when combined with OTP-intercept techniques.

Phishing and "live-admin" panels allowed threat actors to conduct OTP intercept at leisure.

Downstream Fraud Activity:

AI tools likely enabled threat actors to bypass identity processes and conduct synthetic identity fraud more effectively.

Account acquisition tutorials empowered threat actors to conduct fraud and money laundering activity with stolen or forged data.

Sophisticated money laundering services and workflows facilitated fraud activity.

Recorded Future®

Figure 1: *Our research in 2024 offered insights into how threat actors stay ahead of financial institutions' anti-fraud strategies (Source: Recorded Future)*

Magecart E-skimmer Infections Soar after the Arrival of a New Vulnerability and New E-skimmer Kits and the Development of New Tactics

Throughout 2024, Magecart e-skimmers clearly remained effective as a method of data theft. Altogether, the volume of unique e-commerce domains suffering from newly detected e-skimmer infections approached 11,000 — a near-threefold increase from 2023 and the highest ever observed in a single year. Magecart e-skimmer infections occur when threat actors targeting e-commerce websites implant malware on e-commerce websites to steal customer data from payment forms on checkout pages. E-skimmer infections raise financial fraud risks for victims who transact at infected websites.

This year, three primary factors redefined the Magecart threat landscape:

- Beginning in October 2024, infection volume soared due to "CosmicSting" (CVE-2024-34102), a new vulnerability that affects e-commerce websites using Adobe Commerce and Magento
- Threat actors leveraged the advantages offered by "out-of-the-box" e-skimmer kits that lower barriers to entry for Magecart operators lacking technical expertise
- Magecart TTPs continued to develop, contributing to more sophisticated, undetectable, and productive Magecart e-skimmer infections

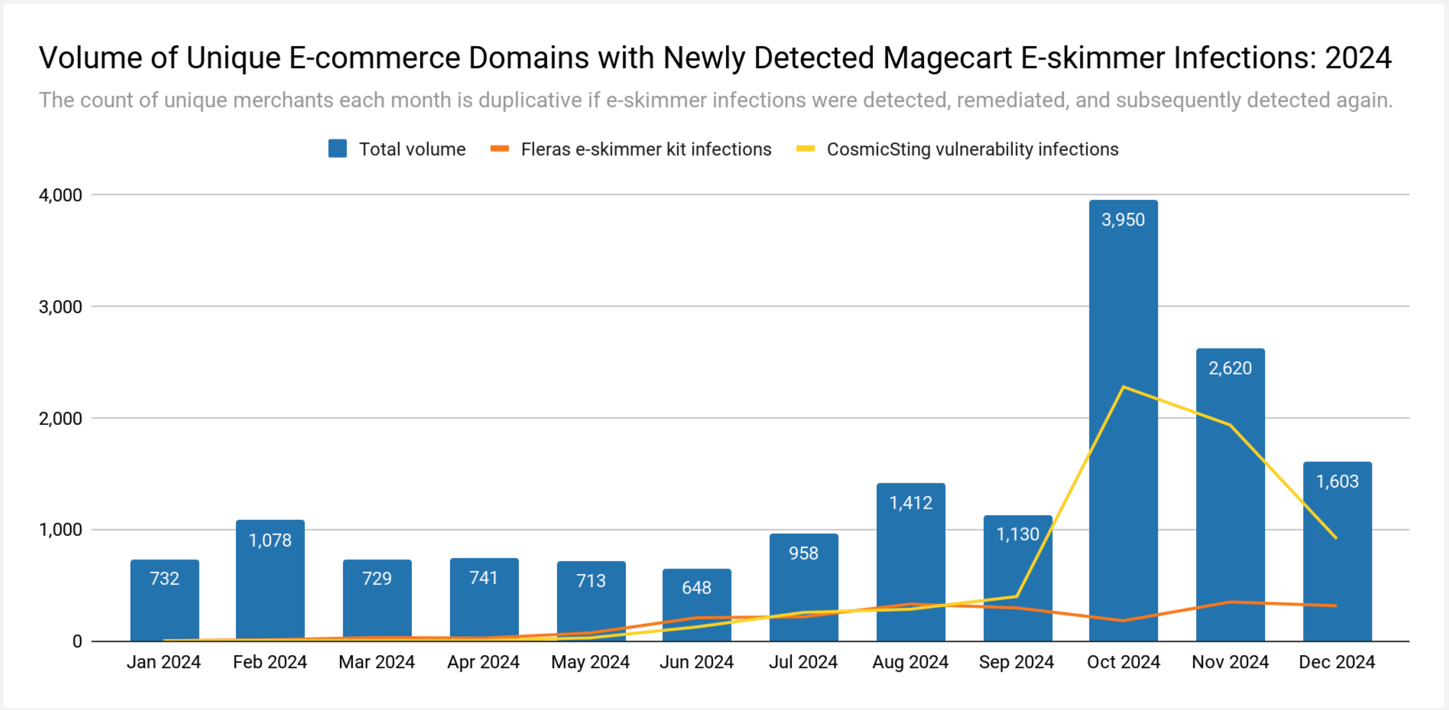


***Figure 2:** Magecart e-skimmer infections that relied on e-skimmer kits — specifically "Sniffer by Fleras" — occupied a growing share of total infection volume until October 2024, when total infection volume soared due to CosmicSting (Source: Recorded Future)*

In Late 2024, CosmicSting Redefined the Magecart Threat Landscape

In late 2024, Magecart Overwatch — Recorded Future's proprietary Magecart e-skimmer scanner — detected an unprecedented increase in Magecart infection volume, which was the result of widespread threat actor exploitation of a newly identified vulnerability: CVE-2024-34102, also known as CosmicSting. Adobe submitted CosmicSting to the US National Vulnerability Database in June 2024. By July 2024, Sansec had observed mass exploitation of the vulnerability in the wild.

Beginning in October 2024, CosmicSting drove a massive spike in our detected infection volume. Since then, indicators of compromise (IOCs) on e-commerce domains infected via the vulnerability have rapidly changed, suggesting that Magecart operators are edging out competing Magecart groups' infections on vulnerable websites. This also indicates that the CosmicSting vulnerability is not being patched by e-commerce website administrators, allowing malicious actors to continue exploiting it to gain access to the websites.

Major E-skimmer Kit Sees High Adoption, Lowering Technical Barriers for Magecart Threat Actors

By September 2024, new Magecart e-skimmer infections using "Sniffer by Fleras", a robust e-skimmer kit developed and marketed by the threat actor "Fleras", had grown to occupy 25% of all new infections since its introduction earlier in the year. This demonstrates the advantages of scale and deployment that e-skimmer kits offer Magecart threat actors lacking technical expertise. Sniffer by Fleras saw substantial use proportionate to all infections until October, when threat actors began exploiting CosmicSting en masse.

While Sniffer by Fleras was the most salient e-skimmer kit this year, others also saw widespread use. The R3nin kit — notable for its simplified command-and-control panel — saw continuing use despite its creator's disappearance in 2023. InterKit remained a mainstay among Magecart groups, and its source code has grown common in many e-skimmer infections.

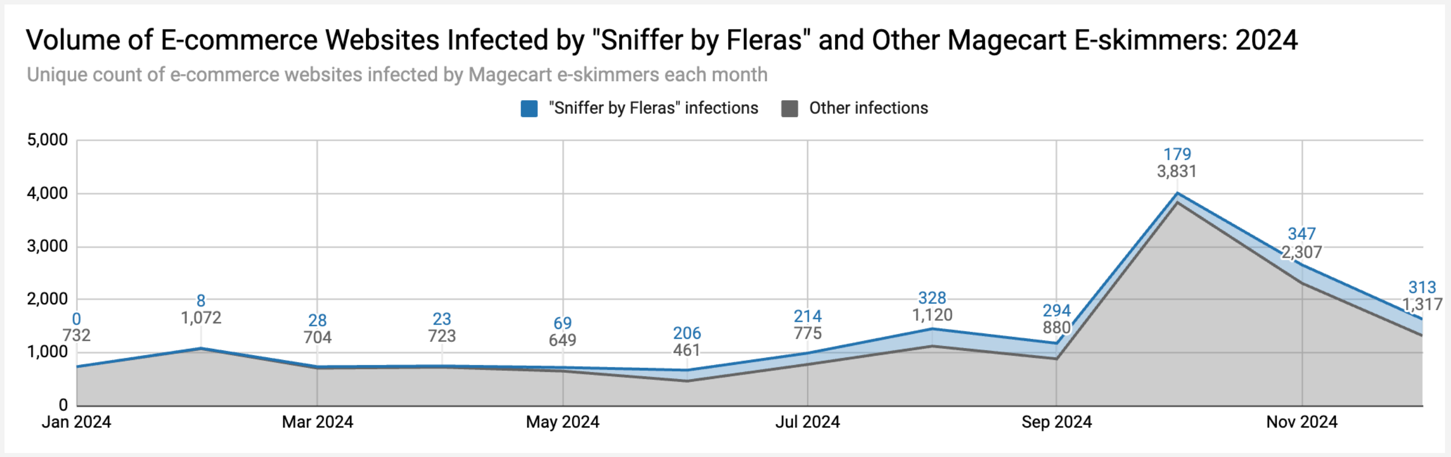


Figure 3: *"Sniffer by Fleras" infection volume this year signified the advantages of e-skimmer kits (Source: Recorded Future)*

Magecart TTPs Continue Evolving, Facilitating Higher Fraud Impact

Our analysis surfaced emerging TTPs among Magecart groups in 2024, which were likely effective. These TTPs demonstrated growing sophistication among Magecart operators while facilitating increased impact, ultimately enabling Magecart e-skimmers to steal customer data from payment forms on infected e-commerce websites more effectively.

- **OTP Intercept:** The Magecart group "OTPExplorer" incorporated a novel intercept technique for victim one-time passwords (OTPs) in its e-skimmer infections, likely to facilitate mobile wallet fraud. This is our first observation of such a technique among Magecart threat actors. Our analysis of dark web discourse indicates that similar techniques demonstrate a high degree of success when employed by scam and phishing website operators.
- **Sophisticated Obfuscation:** The Magecart group "Shablon" employed a novel obfuscation technique to evade detection. The technique involved unpacking a randomly ordered alphabet into variables, which were combined to reconstruct keywords and other script elements.
- **Custom Payloads for Targets:** The Magecart group "Dispatcher" used loader scripts communicating with relays in order to obtain e-skimmer payloads hosted on separate attacker domains, essentially allowing the relay to dispatch e-skimmers built specifically for the target e-commerce websites. These relays likely used the referrer header to identify the victim website and determine which e-skimmer to send.

Despite the emergence of new Magecart TTPs, established TTPs also appeared to remain effective.

- **Abuse of Legitimate Services:** The Magecart group "ADSWG" abused two publicly available web services — Google Tag Manager (GTM) and Amazon CloudFront — as attack infrastructure. The group's e-skimmers used GTM containers housing loader scripts, which injected e-skimmer URLs hosted on Amazon CloudFront distribution subdomains into infected e-commerce websites. This abuse of legitimate infrastructure likely enabled ADSWG to achieve a platform breach targeting an e-commerce platform for online jewelry retailers. Similar to ADSWG, the Magecart group "FakejQuery" implanted links to Trojanized GTM containers into the main page of targeted merchants' infected e-commerce websites.
- **Abuse of Legitimate E-commerce Domains:** The Magecart group "Megaebun" remained active in 2024. In many cases, Megaebun infections used e-skimmer URLs hosted on compromised "attack-carrier" domains belonging to legitimate e-commerce websites.

Scam Websites with Linked Merchant Accounts Grew Rapidly as a Threat

Scam e-commerce websites became a more salient fraud threat in 2024, as indicated by the sheer volume of identified scam websites, linked merchant accounts, and the increasing subtlety and sophistication of scam website TTPs. This trend is equally evident from scam website operators' growing success in defrauding their victims: Better Business Bureau reported that as of June 2024, victims have grown more susceptible to online shopping scams and are reporting more financial losses from them. The growing threat posed by scam websites with linked merchant accounts and payments-based cash-out mechanisms illustrates threat actors' growing recognition that social engineering and secure payments technologies can enable them to bypass anti-fraud defenses.

For financial institutions whose customers are defrauded by scam e-commerce websites, detecting and blocklisting merchant accounts linked to scam websites is likely an insufficient remediation. Scam e-commerce websites incorporating scam merchant accounts enable threat actors to achieve "double monetization": first, through an immediate fraudulent transaction on the scam website, and then again via downstream fraudulent transactions or through the sale of the transacted data on dark web sources.

Most Scam Merchants in 2024 Registered in the United Kingdom and Hong Kong

More than half of the scam websites we identified this year used merchant accounts based in the United Kingdom, and nearly one in five scam merchants were based in Hong Kong. In total, we identified 1,191 scam websites linked to merchant accounts using 767 unique merchant names and 474 unique merchant identification numbers (MIDs).

Threat actors often link scam merchant accounts to clusters of scam websites. In 2024, one such scam merchant account incorporated "JUYUE" into its merchant name and used the MID "3792972NCoYIu50". We linked JUYUE to over 4,000 for-sale card-not-present (CNP) records posted for sale on a dark web marketplace in September 2024. Our research had linked multiple scam e-commerce domains to JUYUE no later than August 27, 2024, three days before MalwareTips independently reported the scam network.

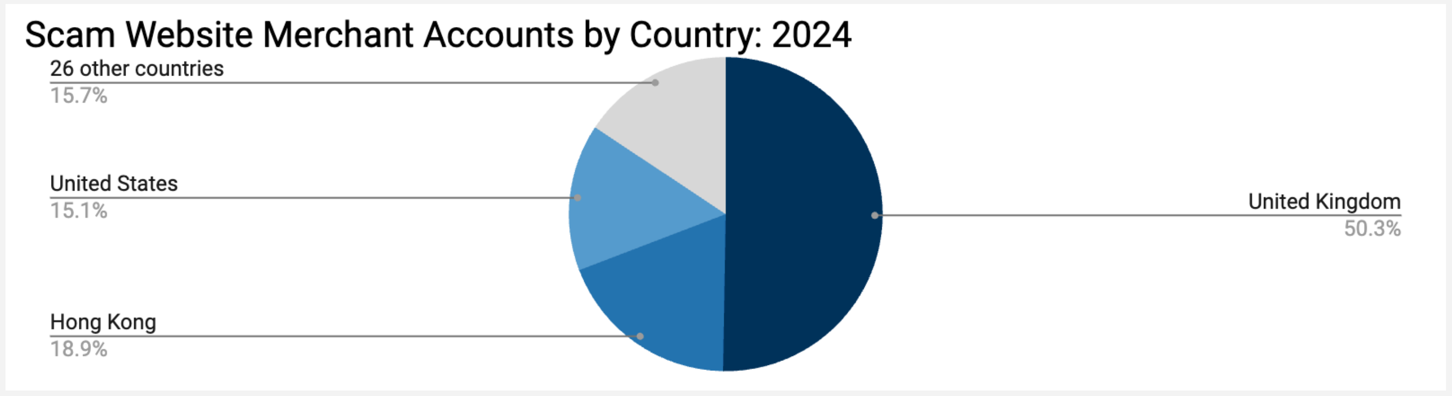


Figure 4: *Nearly three-quarters of all identified scam merchants in 2024 were registered in the UK or Hong Kong (Source: Recorded Future)*

Scam Website TTPs Grow More Subtle and More Sophisticated

This year, major scam website operations used tactics that epitomized the increasing sophistication and subtlety of merchant-linked scam website operations:

- **Victim Screening to Avoid Detection:** "ERIAKOS" screened visitors to its scam websites based on whether they were using a mobile device and whether they had accessed the website via a social media ad lure, likely to avoid detection by online advertising services' static detection rules. As is typical for scam website operations, ad lures linked to ERIAKOS scam websites employed brand impersonation and malvertising to attract victims on social media networks.
- **OTP Intercept:** Similar to OTPExplorer, threat actors associated with a scam website campaign operated by the threat actor "Chenlun" successfully employed OTP-intercept techniques to facilitate real-time fraudulent digital wallet provisioning attempts. Attacks linked to this group were multi-stage, combining smishing communications with scam websites to steal victim data and defraud victims, a tactic that a previous Chenlun-linked operation employed successfully for scam websites modeled after national postal service websites.
- In late 2024, the MailTzz scam website network moved away from the use of linked merchant accounts toward **phishing-based OTP-intercept techniques** that also enabled the scam operators to fraudulently provision stolen card data to digital wallets. This tactical shift occurred amid the broader strategic pivot toward digital wallets as a core cash-out mechanism.
- **Transaction Laundering and Merchant Rotation:** 2024 witnessed increasing reliance among scam operators on transaction laundering and merchant rotation to avoid detection. Transaction laundering and merchant rotation allow scam operators to obscure fraudulent transactions and mask high-risk transactions by redirecting transactions through unrelated websites.

Despite the evolution of the scam website threat landscape, scam website operators in 2024 continued to demonstrate extraordinary sensitivity to seasonal opportunities when preparing and executing their operations. Scam e-commerce websites often leverage seasonal opportunities to take advantage of increased victim susceptibility and raise urgency, usually through fictitious promotional offers. In November 2024, Visa Payment Ecosystem Risk and Control identified a 284% increase in the volume of scam websites compared to the preceding four months. In December 2024, TransUnion indicated that more than 4% of transactions conducted between Thanksgiving and Cyber Monday were suspected to be fraudulent, which was likely driven by both scam activity and more generalized fraud activity.

CPP Analysis Underlines Established — and Emerging — Breach Trends

Transaction analysis conducted with financial institutions allows us to identify and analyze common points of purchase (CPPs), which are often sources of stolen victim financial and personal data. In 2024, we collaborated with partner financial institutions to identify 788 unique CPPs.

Throughout 2024, our analysis of trends in CPPs pointed to an evolving threat landscape. Long-standing trends, such as the preeminence of restaurants among breached merchants or the elevated threat posed by platform breaches compared to small-scale breaches, remain evident in the data. At the same time, the increasing prominence of fashion stores among CPPs was largely driven by increases in identified scam merchant CPPs, highlighting threat actors' shift toward scam websites across the year.

The frequency of restaurants as a CPP merchant category was largely driven by US fraud trends, where restaurants and bars remain vulnerable to card-present breaches. This vulnerability arises from restaurants' and bars' centralized point-of-sale (POS) systems, which servers use to transact customer cards out of the customer's view. This dynamic presents unscrupulous staff members with an opportunity to steal card data using pocket skimmers. More surprising this year was the preeminence of fashion stores among CPPs in 2024, which was driven by scam e-commerce trends. Scam websites often purport to offer discounted clothing for sale. In 2024, 38% of all CPPs we identified with merchant category code (MCC) 5621 and 39% of all CPPs with MCC 5691 were confirmed scam merchants.

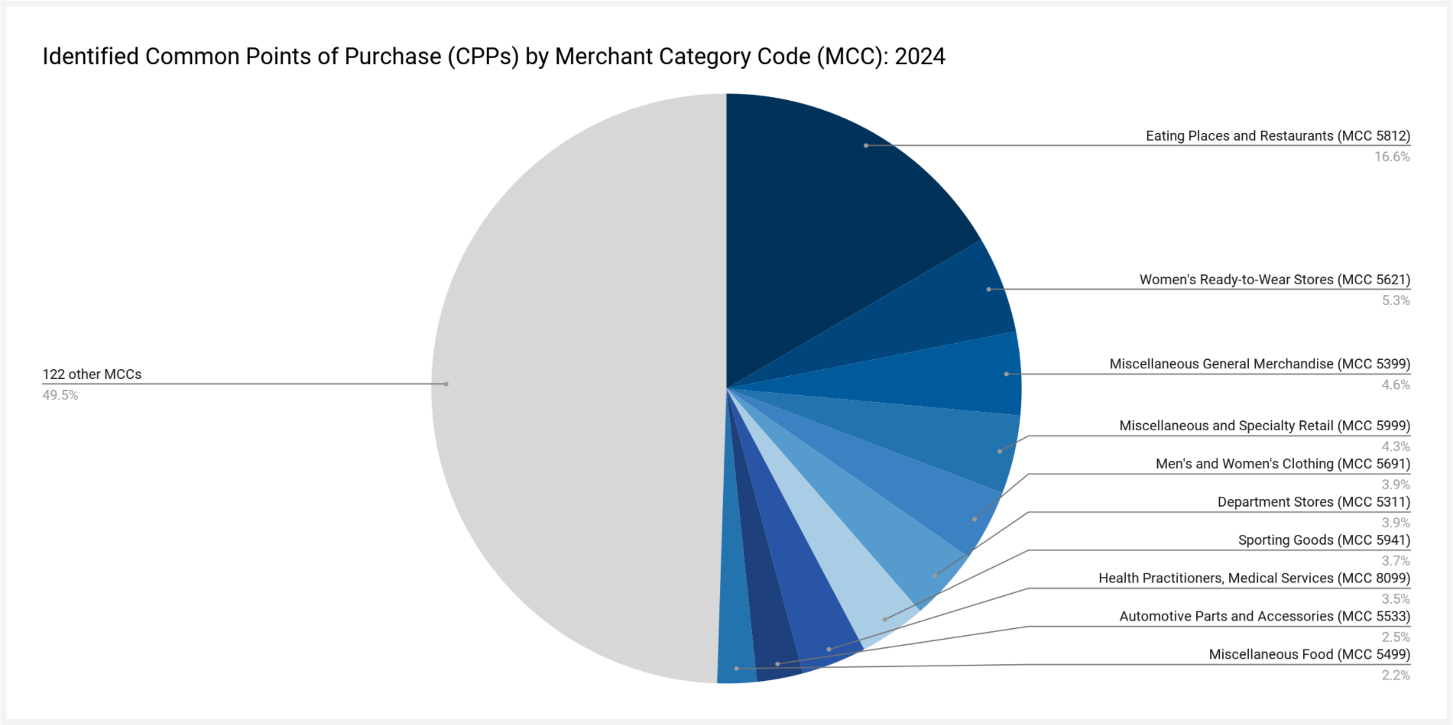


Figure 5: *Most CPPs this year were restaurants, although scam trends drove fashion stores into the top ten MCCs by volume of CPPs (Source: Recorded Future)*

Among CPPs, platform breaches continued to present a major threat to e-commerce in 2024. Platform breaches are highly impactful because a breach of an e-commerce platform used by multiple merchants can potentially compromise all customer transactions with merchants using that platform.

Our analysis of Magecart e-skimmer data and CPP data allowed us to identify two likely major platform breaches in 2024:

- **67 e-commerce websites using a US-based e-commerce platform catering to jewelry retailers were infected with Magecart e-skimmers as of July 2024.** The ADSWG Magecart operators likely compromised the merchants by infecting a centralized code repository or by using breached admin credentials to manually infect the merchants.
- **A US-based e-commerce platform catering to restaurants was likely compromised in late 2024.** Magecart threat actors injected an e-skimmer infection into a file hosted on the platform's content delivery network, indicating that all restaurants using the platform were highly likely to have been impacted by the breach. As of this writing, transaction analysis in collaboration with financial partners has linked approximately 50 merchants using the platform to for-sale card records on the dark web. It is worth noting that hundreds of merchants appear to use the platform.

Volumes of Freely Posted and For-Sale Card Data Surge Throughout 2024

The availability of victim card and cardholder data surged in 2024, with 269 million card records posted on dark web and clear web sources. This was especially true of for-sale card data on dark web marketplaces, with 70 million more card records published for sale compared to 2023. The count of dark web sources from 2023 to 2024 was largely unchanged, and the volume of records posted for sale each month was consistently high and distributed across sources, suggesting the increases likely occurred simply because dark web vendors acquired more stolen cards.

While the increased availability of stolen for-sale card data may have defined the year, the implications of the surge remain unclear. For example, it is possible that the actual fraud risk of for-sale card data may not have increased commensurately with the year's spike in volume. Nevertheless, the increased availability of for-sale card data was likely a function of both increased card compromise events and more frequent reposting within the carding ecosystem. Analysis indicated that the share of for-sale card data that was likely reposted or recycled from other sources rose from 19% in 2023 to 36% in 2024, while the share of data that was likely new and unique nearly doubled in the same period.

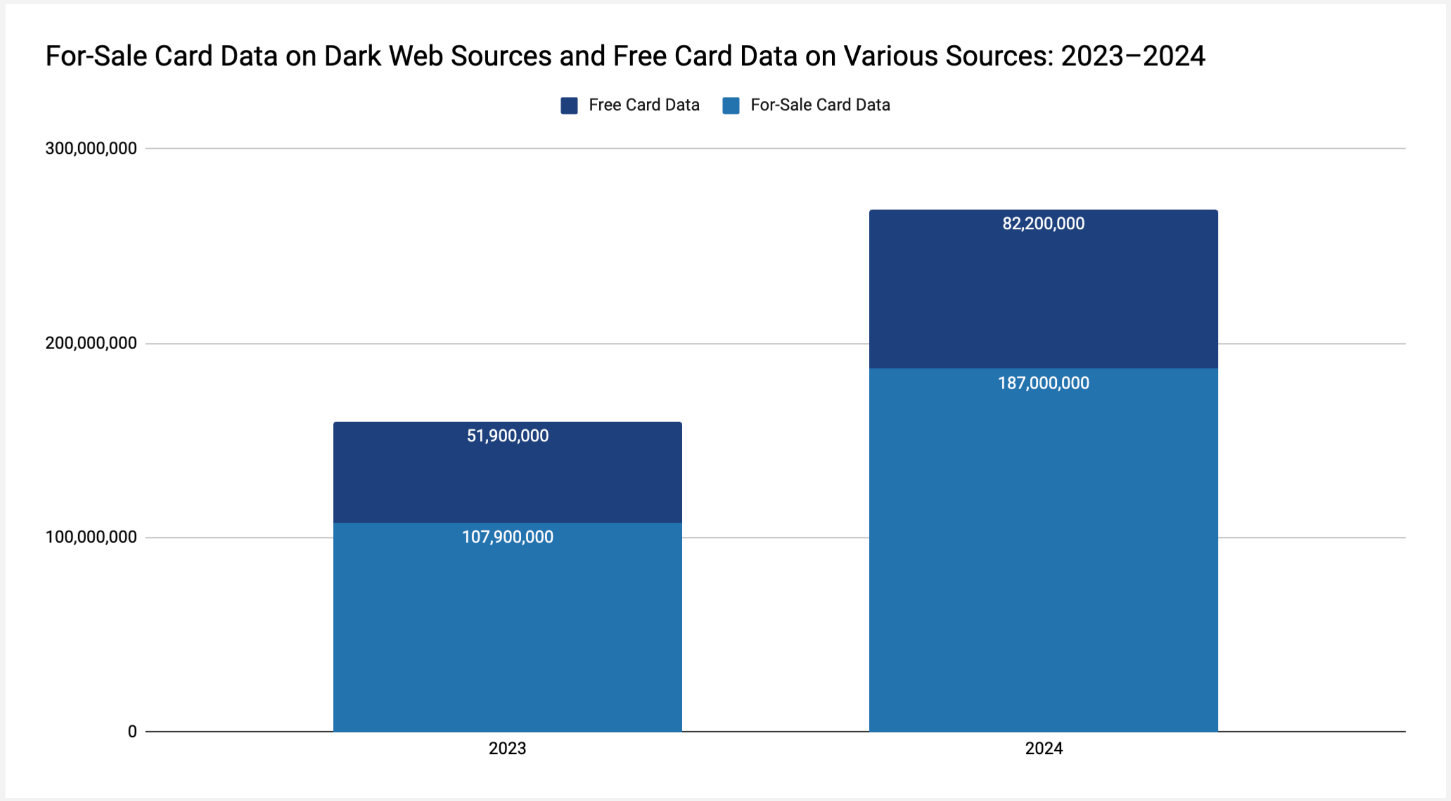


Figure 6: *The volume of free and for-sale card data spiked in 2024, and our analysis indicated the increase in for-sale cards was likely due to both increased card compromise and reposting on dark web sources (Source: Recorded Future)*

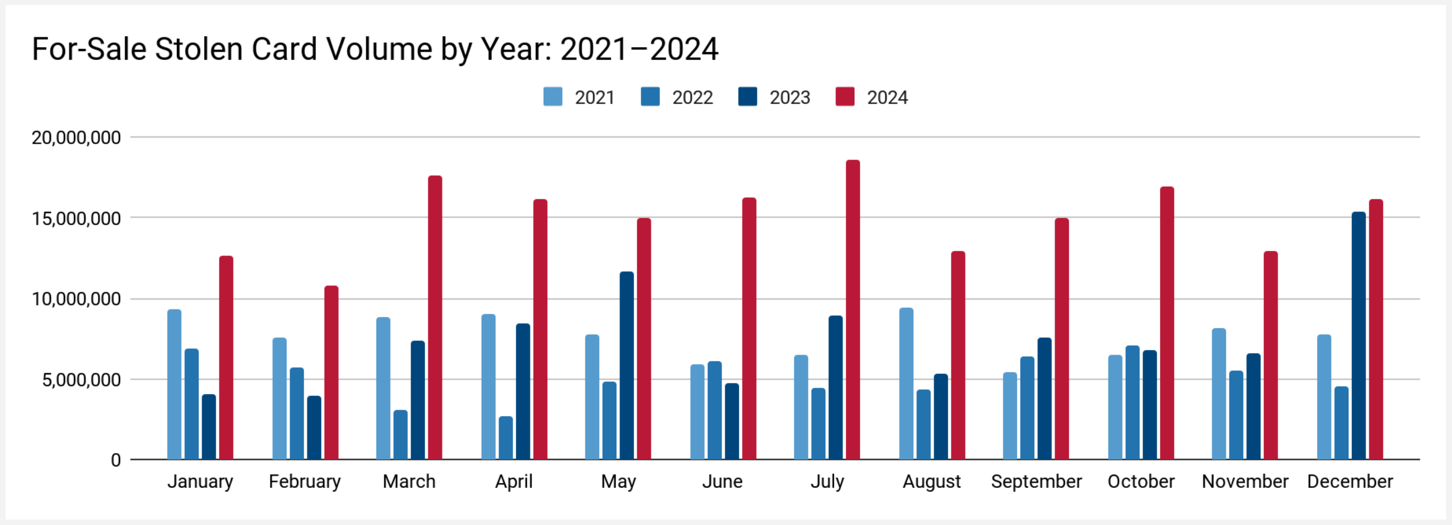


Figure 7: *On a month-to-month basis, the volume of data posted for sale on dark web sources was consistently high, suggesting that the year's increase was simply a result of vendors stealing more card records (Source: Recorded Future)*

Victim data stolen via CNP transactions and malicious online activity — for example, through compromised e-commerce transactions, phishing, and infostealer infections — continued to comprise the vast majority of compromised card and cardholder data in 2024. Seven out of eight for-sale card records on the dark web this year were CNP, and practically all freely available card data was CNP.

Despite the diminished exposure of CP data — which itself is the result of improved physical transaction security technology and the growing share of e-commerce in the retail sector in recent years — our analysis confirmed CP fraud schemes likely continue to remain in play, though scarce. Our investigation of dark web sources this year surfaced multiple CP fraud workflows and services relating to card skimming, card shimming, POS malware, and card cloning, which likely remain effective.

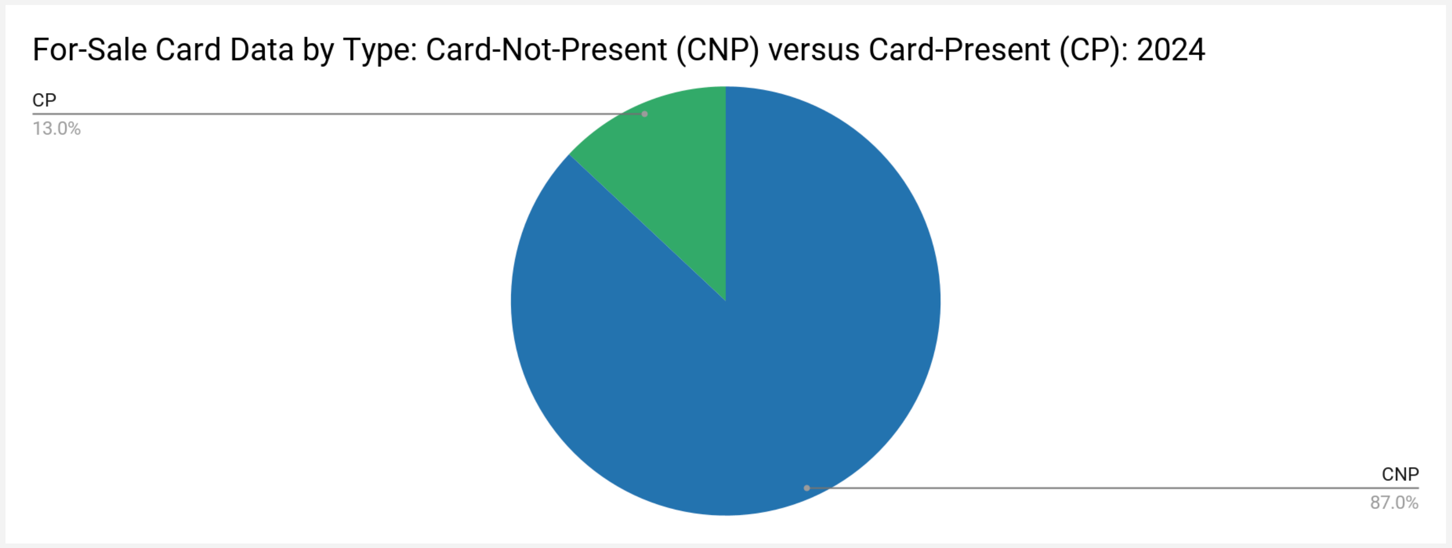
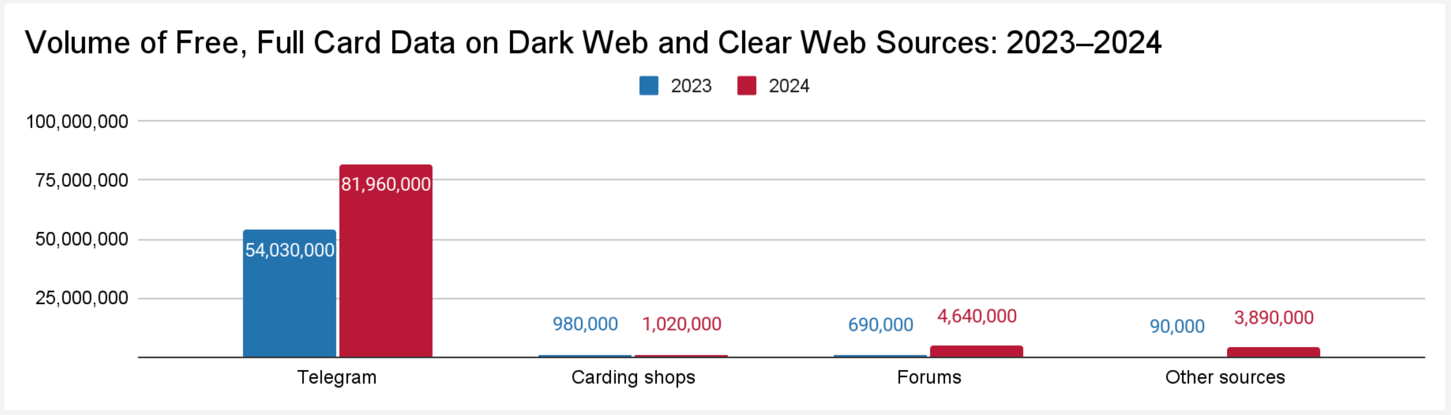


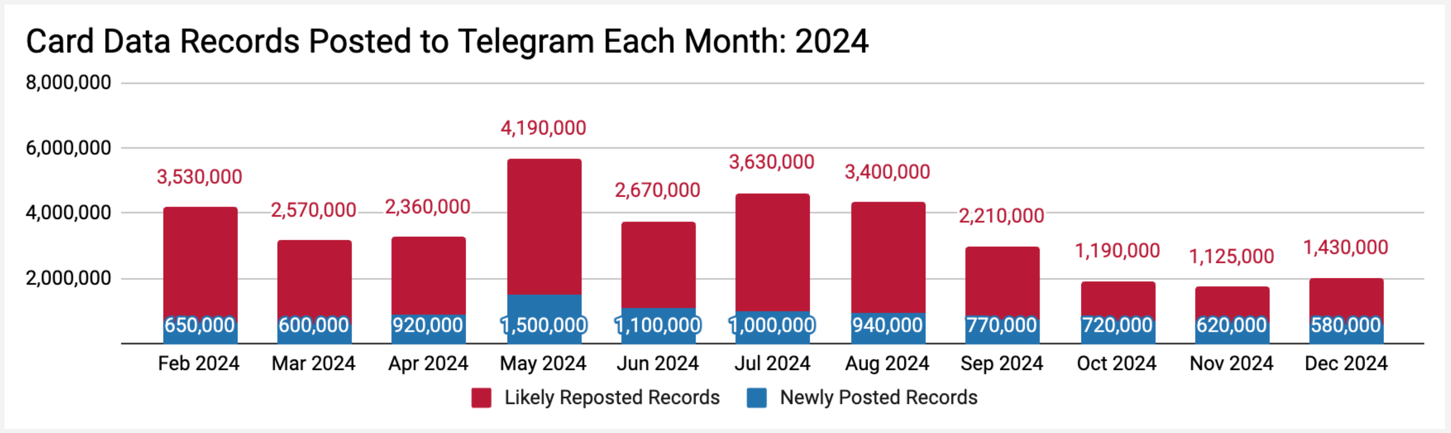
Figure 8: *In 2024, seven out of eight stolen cards posted for sale on dark web marketplaces originated from CNP transactions and malicious online activity (Source: Recorded Future)*

This year, the dark web fallout following law enforcement's disruption of criminal payment infrastructure briefly threw the dark web carding underground into disarray but also demonstrated its resilience. The disruption of this infrastructure was announced alongside the indictment of Timur Shakhmametov, the operator of the notorious, now-defunct dark web marketplace Joker's Stash. As a consequence, BriansClub — a major source of for-sale card data in the wake of Joker's Stash's closure — was forced offline to pivot to new infrastructure and safeguard its operations. BriansClub reopened after a month-long hiatus.

Trends on Telegram — long a hotbed of fraud-focused activity — primarily drove the increase in sources of free card data we identified in 2024, even as the per-source volume of data on Telegram dropped. The arrest of Telegram's founder, Pavel Durov, and Telegram's subsequent agreement to furnish user ID data to authorities heralded a decrease in the total volume of card records posted on Telegram sources beginning in September 2024. Despite overall falling volumes following Telegram's concession, the total quantity of new, unique records posted on Telegram remained stable, indicating the source will likely continue to be used for fraud in the near future.



Volume of Free, Full Card Data on Dark Web and Clear Web Sources: 2023–2024



Card Data Records Posted to Telegram Each Month: 2024

Figures 9 and 10: *Despite Pavel Durov's arrest, Telegram continued to remain a source of card data in 2024 (Top). While the raw volume of free card data on Telegram dropped beginning in September 2024, following Pavel Durov's arrest, analysis indicated that the volume of new, unique card data likely remained stable (Bottom). (Source: Recorded Future)*

New, unique card data on Telegram was often produced as a result of threat actor efforts to generate and validate card data. Card validation and generation features on Telegram sources support account enumeration attacks, also known as BIN attacks. Throughout 2024 we observed multiple instances of generated records, likely from BIN attacks. A large-scale example occurred on the Telegram channel "Free Worldwide Data", which released a database containing twenty million full card data records. Our analysis with partners revealed that the data included few active and valid records and an unusually even distribution of expiration years. Additionally, none of the records included cardholder personally identifiable information (PII). These factors indicated a high likelihood that the records were generated and — in this case, at least — low-threat.

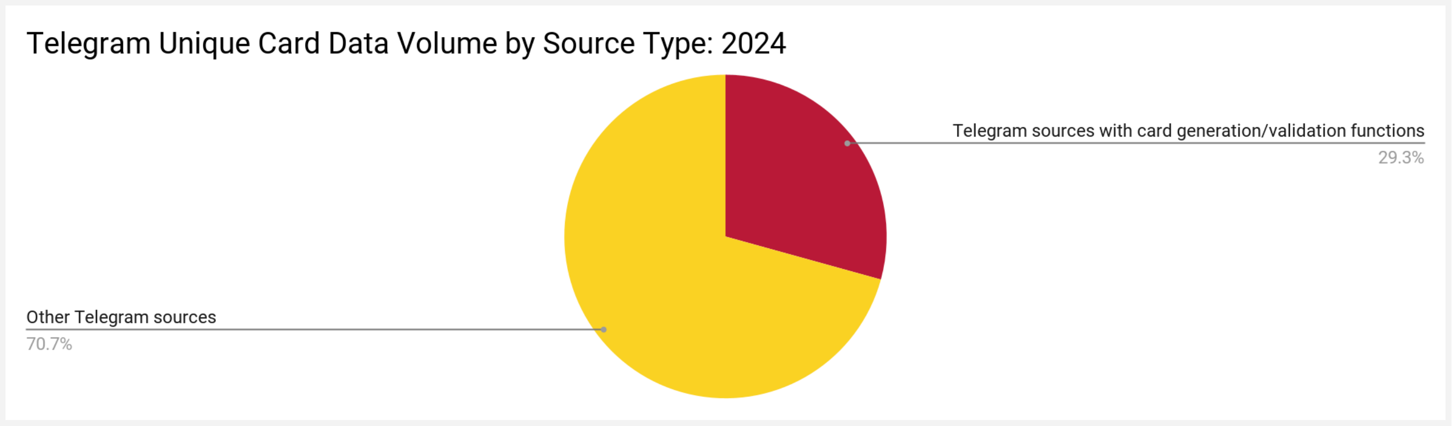


Figure 11: *Sources with card generation and validation functions accounted for a substantial volume of unique card data attributed to Telegram in 2024 (Source: Recorded Future)*

While large-scale data leaks tend to garner media buzz, our observations indicated that the largest card data dumps in 2024 tended to pose the lowest direct fraud risk:

- **In January, the threat group "KibOrg" released over 40 million card records on its eponymous Telegram channel.** The database was allegedly stolen from the Russian financial institution Alfa-Bank.
- **In April, the source "b1ack's Stash" released two databases totaling over one million CNP records**. Most of the data in this release did not contain cardholder address information, decreasing threat actor's expected success rates while monetizing the card information.
- **In May, the source "BidenCash" released a database of four million full card records, part of a continuing promotional tactic**. These records were likely previously posted for sale or for free, and likely posed a low fraud threat.
- **In July, the threat actor "ShinyHunters" released a database with nearly thirteen million transaction records, which contained over two million unique partial card data records**. The records appeared partially tokenized, vastly reducing their fraud attack surface.
- **In August, the threat actor "Fenice" shared over two billion lines of data from the National Public Data breach.** While the data could serve as a lookup table to support fraud activity, it likely presented a low direct fraud threat.

Tester Merchant Analysis Indicates More Checkers and Short-Term Abuse

Dark web checkers offer card validation services to carding shops and threat actors through application programming interfaces (APIs), purpose-built websites, and Telegram bots. Together with partner financial institutions, we identify and analyze tester merchants used by checkers to validate stolen payment cards. In turn, this tester merchant data offers useful signals that financial institutions can use to identify at-risk card accounts.

Checker-originated card validation activity increased in 2024 and is likely to increase in 2025, as indicated by increases in the quantity of checker services throughout the year. The number of tester merchant names surfaced through our research dropped compared to 2023. This was almost certainly a result of the closure of Try2Check in May 2023, which had devised a means to rapidly alter tester merchant names for the same merchant account. Meanwhile, the number of identified tester MIDs increased by 48%, highlighting the growing availability of merchant accounts for card validation abuse.

Year	Identified Tester Merchant Names	Identified Tester MIDs	Checkers
2022	2,953	660	20
2023	1,618	684	27
2024	914	1,010	42

Table 1: *In 2024, the total count of dark web checkers and tester merchant MIDs increased, pointing to heightened card validation activity (Source: Recorded Future)*

Dark web checkers preferred abuse of tester merchants over short-term, non-consecutive periods of time against prolonged consecutive abuse, likely to avoid detection by financial institutions. A minority of all MIDs abused for card validation were abused for consecutive periods lasting longer than one month, and only 52 MIDs were abused for consecutive periods lasting longer than three months. Infrequently, checkers returned to previously abused tester merchants after a “cooldown” period.

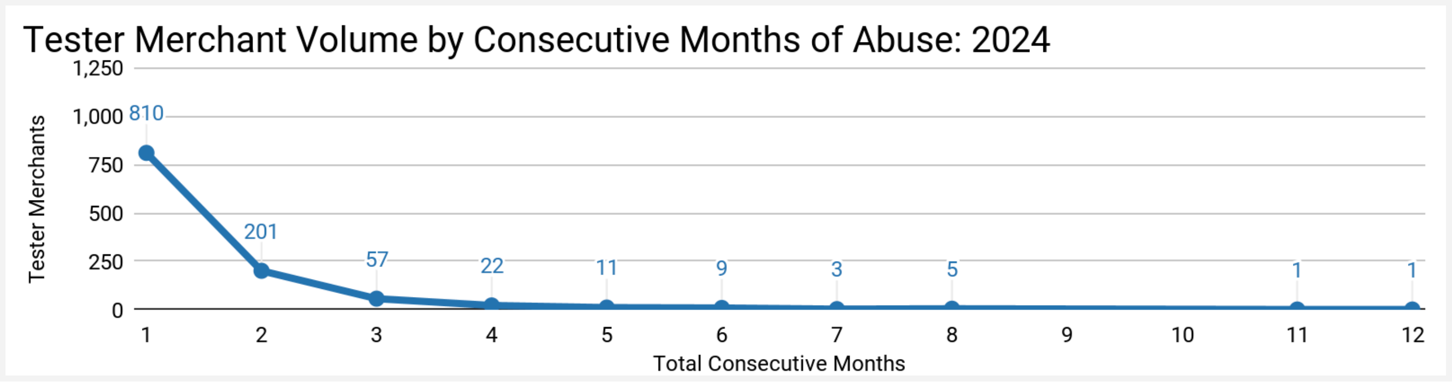


Figure 12: *Checkers most frequently abused MIDs for one month at a time, and far fewer abused MIDs for two or more consecutive months (Source: Recorded Future)*

Most tester merchants in 2024 tended to be from a cluster of merchant categories. Among the more than 150 MCCs associated with abused tester merchants in 2024, the top five MCCs comprised more than a third of all tester merchants. Our analysis indicates that these MCC trends likely reflect the access methods commonly used by threat actors to abuse legitimate merchant accounts for card validation activity. For example, many restaurants (MCC 5812) have poor cyber hygiene, likely enabling their merchant accounts to be abused for card testing. Other access methods include abuse of publicly facing payment forms and illicit access to APIs through API keys traded on the dark web. Dark web discourse this year indicates that the growing illicit trade of API keys will likely increase the scale of testing activity throughout 2025.

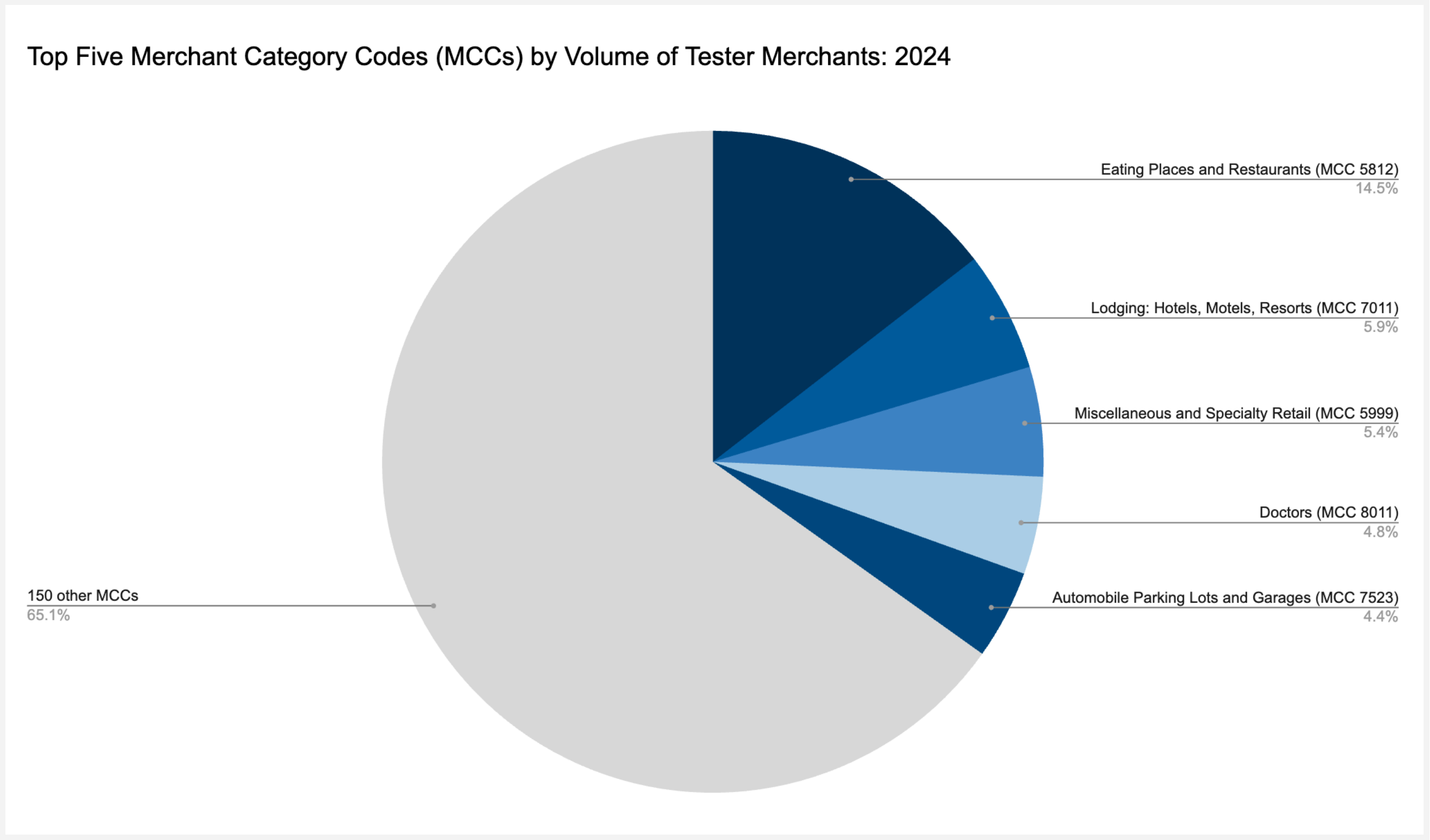


Figure 13: *The top five MCCs for tester merchants abused in 2024 comprised a third of total tester merchant volume (Source: Recorded Future)*

Massive Reposting and Geography Shape the Check Fraud Threat Landscape

Check fraud is a uniquely US phenomenon. Our analysis indicated that rampant reposting and geographic trends define the check fraud threat landscape. Approximately nine out of ten stolen check images in 2024 existed as reposts of unique data on other sources. Altogether, 190,000 unique stolen checks dated in 2024 were posted for sale, with 1.9 million total check images (including reposts) offered for sale. While frequent reposting suggests that the raw volume of stolen checks does not accurately represent the scale of the check fraud threat, reposting nevertheless expands the fraud attack surface for exposed checks.

Analysis of available payer geographic data for stolen checks this year indicated two major trends:

- **The US East Coast is disproportionately affected by check fraud.** For perspective, the US East Coast holds 35% of the US population but originated 60% of stolen checks for the year.
- **Checks from certain US states are reposted more frequently than checks from other states, suggesting there may be increased demand for check data in certain states.** For all US states, repost rates ranged from 77% (Wyoming) to 93% (West Virginia).

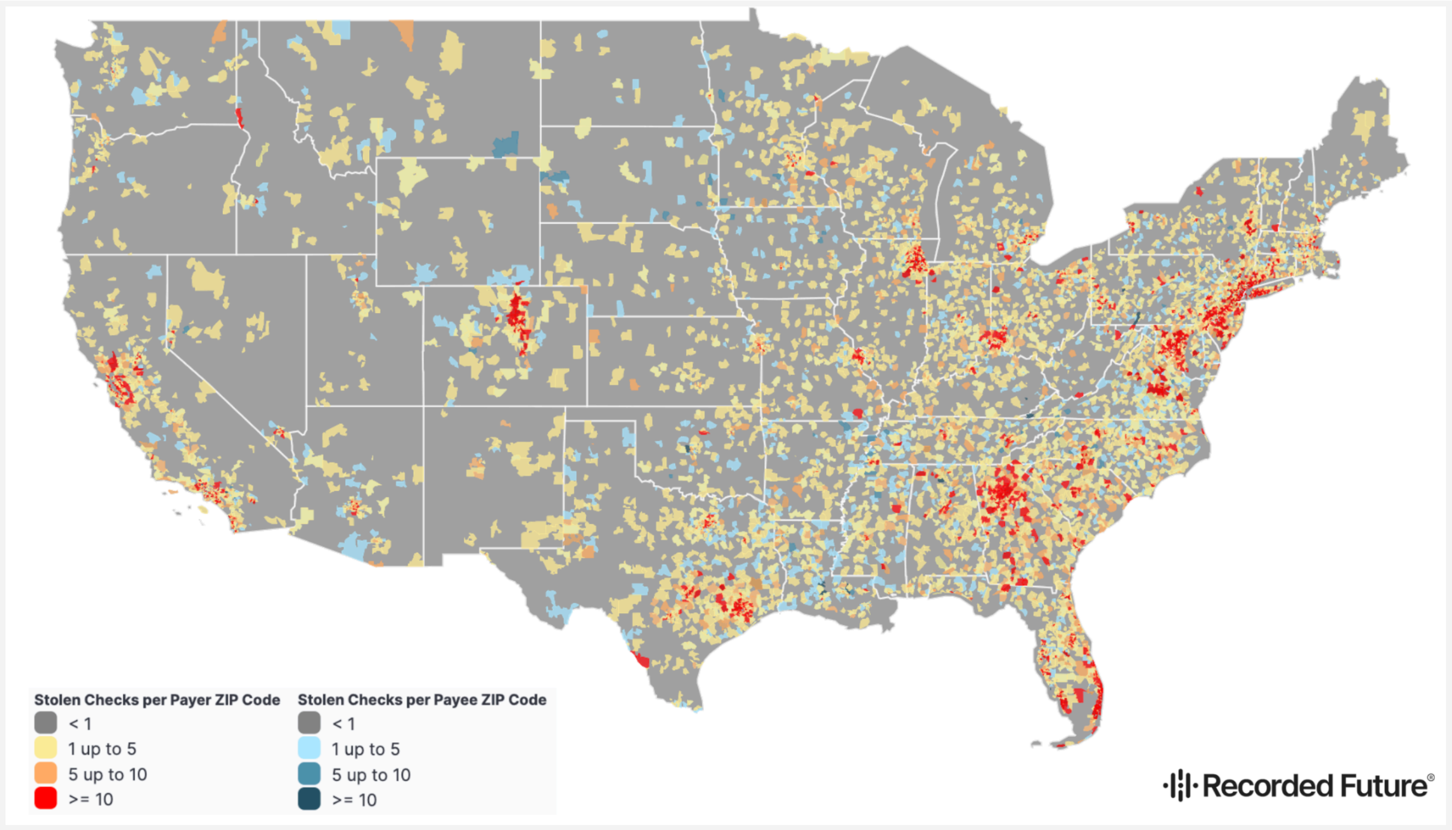


Figure 14: *The US East Coast is disproportionately impacted by check fraud (Source: Recorded Future)*

Dark Web Discourse Indicates Growing Sophistication Drives Fraud TTPs

In 2024, a major theme that emerged in dark web fraud-focused discourse was increasing threat actor willingness to subvert and surmount convenience- and security-focused "trust systems" in order to conduct fraud. Customer-facing fraud has always been enabled by threat actors' ability to navigate business rules, but observed fraud workflows this year demonstrated threat actors' desire to embrace the limitations of specific security-oriented technology or even leverage them to their advantage. Selective pressures from effective anti-fraud action likely drove much of this evolution, as did AI enablement.

Many of these developments are detailed in the sections above. More broadly, dark web discourse evidenced this evolution across three categories of fraud activity:

- Subversion and defeat of financial technology to defraud victims
- Nuanced verification bypass workflows for new account fraud, fraudulent acquisition of financial accounts, and synthetic identity fraud
- Continuing reliance on complex money laundering services and tactics

Subversion and Defeat of Financial Technology Meant for Customer Security

Fraud workflows we identified throughout the year demonstrated how threat actors have begun to embrace security mechanisms as fraud mechanisms. This year threat actors demonstrated the willingness and know-how to adapt technologies designed to improve customer security and convenience as fraud cash-out tools.

- **Digital Wallets:** Threat actors largely conduct digital wallet fraud through OTP intercept techniques, although the methods may differ. Phishing and malware are old standbys, although real-time panel-based provisioning gained popularity in 2024. Nevertheless, the two points of success are unchanging: the fraudulent provisioning attempt and the fraudulent transaction.
- **Open Banking Applications:** High-threat workflows enable threat actors to cash out compromised bank accounts through financial technology ("fintech") apps meant to increase customer convenience, offering multiple pathways to defund victim accounts. Our previous research indicates that threat actor exploitation of open banking is not novel; this year merely demonstrated a growing refinement in attack methodology.
- **Phishing Panels:** While phishing admin panels are not security technology, they are threat actors' answer to the protections offered by security measures like 3-D Secure (3DS) protocol. Throughout 2024, threat actors like "Simba_Service" offered live admin panels that can facilitate man-in-the-middle OTP intercept attacks to bypass 3DS-protected transactions and enable attacks described in other sections of this report, including those linked to MailTzz.

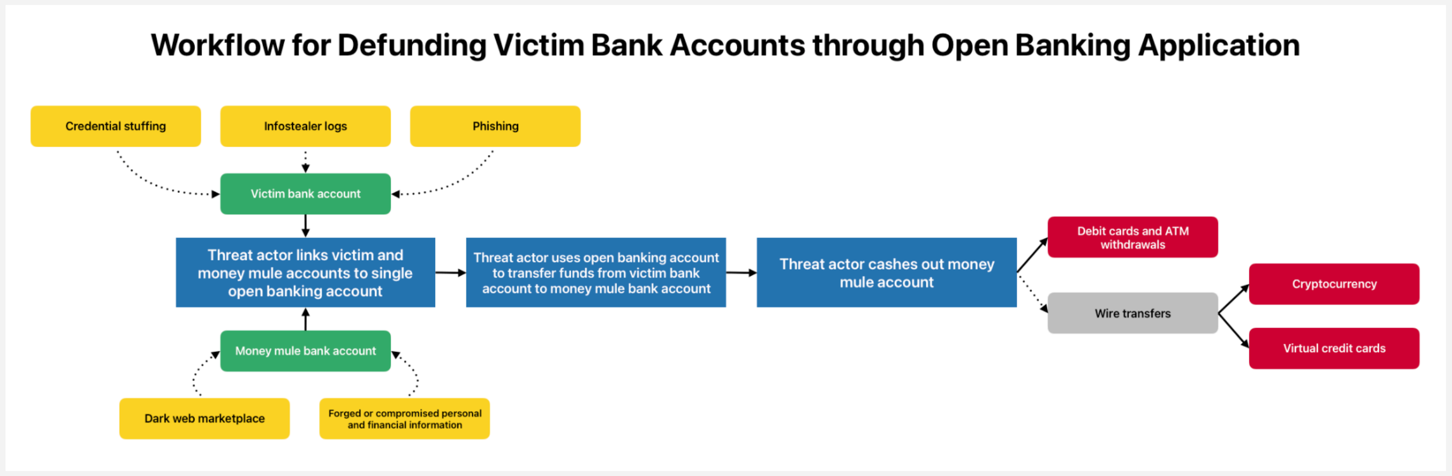

Workflow for Defunding Victim Bank Accounts through Open Banking Application
Credential stuffing
Infostealer logs
Phishing
Victim bank account
Threat actor links victim and money mule accounts to single open banking account
Threat actor uses open banking account to transfer funds from victim bank account to money mule bank account
Threat actor cashes out money mule account
Debit cards and ATM withdrawals
Wire transfers
Cryptocurrency
Virtual credit cards
Money mule bank account
Dark web marketplace
Forged or compromised personal and financial information

Figure 15: *One fraud workflow confirmed that abuse of open banking applications offers threat actors multiple monetization pathways to defund victim accounts (Source: Recorded Future)*

Nuanced Verification Bypass Workflows for Account Acquisition and Fraud

Threat actors demonstrated nuanced verification bypass workflows on dark web sources aimed at fraudulently acquiring financial accounts and defrauding victims. Verification bypass is often an inescapable requirement for fraud workflows. Nevertheless, this year, threat actors leveraged AI enablement and an appetite for complexity when devising bypass flows for identity processes.

- **Fraudulent Account Acquisition for Downstream Fraud:** In spite of improving identity processes, new account fraud continues to enable downstream fraud. One account acquisition tutorial outlined likely effective guidance for bypassing PayPal's verification processes, obtaining a fraudulent PayPal Mastercard debit card account, and using the fraudulent accounts for downstream fraud and money laundering.
- **Business Card Account Acquisition for Immediate Monetization.** Threat actors monitor financial products closely and are quick to create workflows when they sense an opportunity to profit. Using one workflow, threat actors could likely immediately monetize a business card product's accessible credit as well as a promotional gift card tied to account opening.
- **AI-Enabled Synthetic Identities:** Growing adoption of AI technology likely offers threat actors opportunities to forge synthetic identities for downstream fraud and money laundering more effectively — especially when combined with stolen data. A synthetic identity fraud tutorial we analyzed could likely be enhanced using AI technology. Note that the use of AI to forge synthetic identities is likely already occurring.
- **AI-Enabled Verification Circumvention:** The threat ecosystem has a growing desire to fight fire with fire by using AI technology to circumvent AI-enhanced verification processes. A nuanced tax refund fraud tutorial appeared to enable threat actors to bypass ID.me video selfie verification using deepfakes and AI tools. While we could not confirm the effectiveness of this workflow, we also could not confirm whether AI-powered verification processes would be effective in preventing the attack.

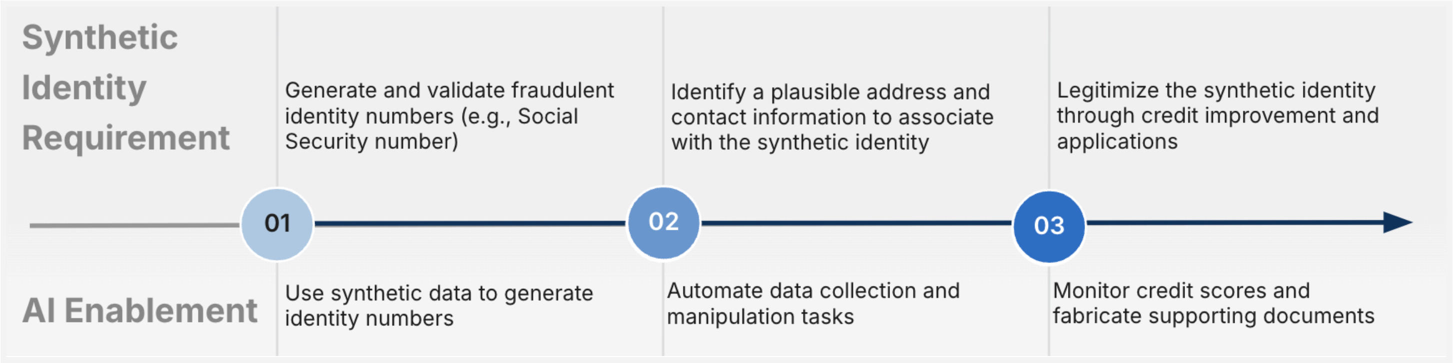

Synthetic Identity Requirement
Generate and validate fraudulent identity numbers (e.g., Social Security number)
Identify a plausible address and contact information to associate with the synthetic identity
Legitimize the synthetic identity through credit improvement and applications
01
02
03
AI Enablement
Use synthetic data to generate identity numbers
Automate data collection and manipulation tasks
Monitor credit scores and fabricate supporting documents

Figure 16: *AI enablement — especially when combined with stolen data — likely improves the efficacy of synthetic identity fraud workflows (Source: Recorded Future)*

Highly Sophisticated Money Laundering Services and Tactics

Law enforcement's disruption of criminal payment infrastructure in 2024 demonstrated how crucial money laundering infrastructure is for fraudsters. This year, threat actors continued to make use of sophisticated cryptocurrency services and complex money laundering workflows to facilitate fraud.

- **Cryptocurrency Mixer and Affiliate Mixers:** Jambler.io uses a sophisticated affiliate scheme to obscure cryptocurrency transactions. The mixer very likely presents an anti-money laundering risk to financial institutions and cryptocurrency exchanges.
- **Confirmed Efficacy:** Three cryptocurrency wallets associated with Exploit Forum have received more than 3,850 Bitcoin (BTC) since 2018, highlighting the source's role as a financial nexus within the cybercrime ecosystem.
- **Transaction Laundering:** By redirecting merchant-based transactions from scam websites and other high-risk sources, threat actors can likely obscure high-risk or fraudulent transactions (see Transaction Laundering and Merchant Rotation above).

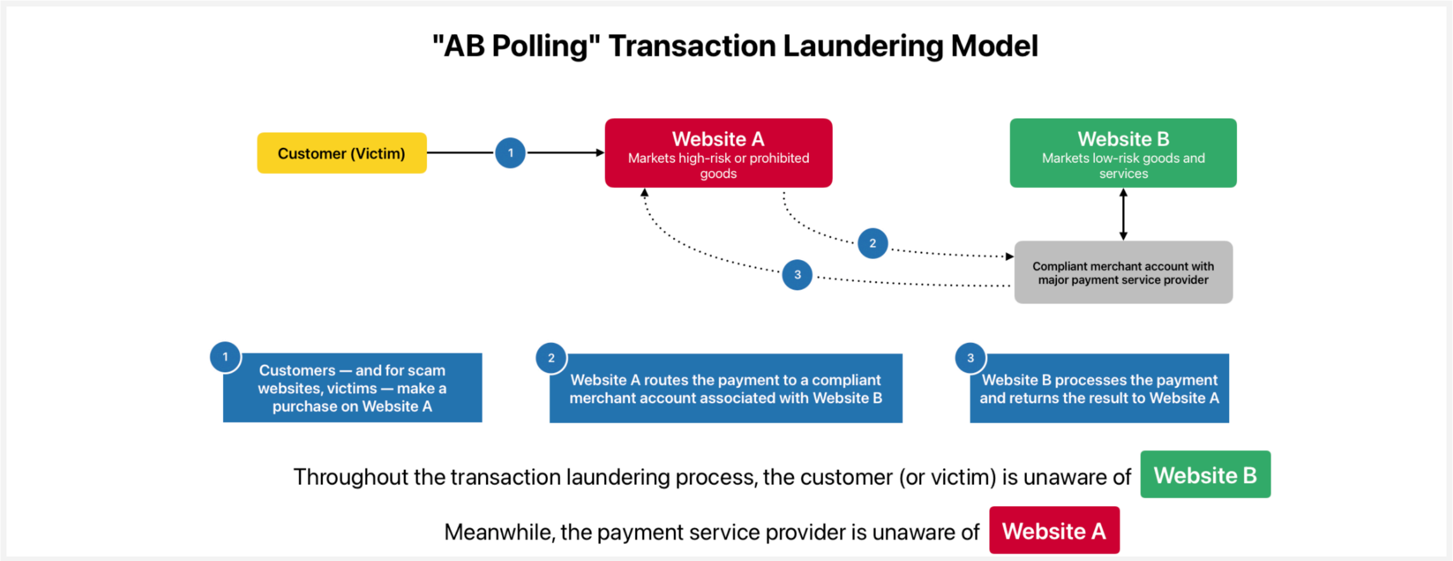

"AB Polling" Transaction Laundering Model
Customer (Victim)
1
Website A
Markets high-risk or prohibited goods
Website B
Markets low-risk goods and services
2
3
Compliant merchant account with major payment service provider
1
Customers — and for scam websites, victims — make a purchase on Website A
2
Website A routes the payment to a compliant merchant account associated with Website B
3
Website B processes the payment and returns the result to Website A
Throughout the transaction laundering process, the customer (or victim) is unaware of Website B
Meanwhile, the payment service provider is unaware of Website A

Figure 17: *Chinese-language sources refer to transaction laundering methods as "AB Polling" (Source: Recorded Future)*

Mitigations

- Encourage acquired merchants to identify and close vulnerabilities on e-commerce websites that threat actors can exploit to implant Magecart e-skimmer infections.
- Increase the rigor of merchant onboarding processes to deter threat actors seeking to fraudulently acquire merchant accounts.
- Enhance validation requirements for digital wallet provisioning attempts. Notify cardholders upon successful provisioning attempts.
- Implement push provisioning through online banking applications. Monitor device indicators for tokenization requests for fraud signals.
- Implement CTI–fraud fusion workflows, specifically through intelligence deliverable-feedback loops that equip CTI and anti-fraud teams to detect and prevent fraud more effectively:

    - Use Recorded Future Payment Fraud card data intelligence to proactively identify and apply appropriate fraud controls to at-risk customer accounts in your portfolio.
    - Use Recorded Future Payment Fraud Magecart e-skimmer intelligence to identify customer accounts that transacted with infected e-commerce websites.
    - Leverage transaction analysis and Recorded Future Payment Fraud CPP intelligence to identify likely breached merchants.
    - Use Recorded Future Payment Fraud tester merchant intelligence to identify merchants being abused for card validation activity.
    - Use Recorded Future Payment Fraud bank check intelligence to identify customer checks or deposits that are likely to be fraudulent. Where able, leverage structured check data to perform check fraud prevention workflows using automation.
    - Use Recorded Future Payment Fraud scam merchant intelligence to identify and blocklist high-risk merchants and identify at-risk accounts.
    - Identify effective fraud workflows on dark web sources and incorporate methodologies to mitigate these attempts at fraud on a recurring basis.
    - For all intelligence deliverables, combine threat landscape metrics and internal inputs to fine-tune fraud strategy.
    - Communicate feedback to intelligence assets to help identify and drive intelligence priorities.

- Continually reevaluate anti-fraud methodology for products or portfolio segments where fraud losses justify additional anti-fraud action. Note that reactive transaction monitoring will likely remain insufficient to minimize your institution’s fraud risk in the long term without the external inputs that intelligence provides.

Outlook

Evolution is expected in any criminal threat landscape, and fraud is no exception. As emerging technologies and investigation flows drive improved anti-fraud systems, threat actors probe financial institutions' defenses for weaknesses that can be exploited to defraud victims. It is, therefore, unsurprising that as financial institutions and other organizations adopt cooperative CTI–fraud fusion strategies to overcome the Castle Dilemma, threat actors increasingly turn to their own "dark-side" fusion strategies to conduct fraud. While trends this year are somewhat superficial against the ever-shifting backdrop of the cyber-enabled fraud landscape — which is itself influenced by constantly changing technological, economic, and regulatory factors — threat actors' ability to adopt security and convenience mechanisms as fraud mechanisms in 2024 nevertheless portends challenges to come.

Looking forward, our analysis of the trends from this report points to three major predictions for 2025:

- **Digital e-skimming and scam e-commerce will drive CNP data compromise events in 2025, especially as fraudsters prioritize digital wallets and fraudulent card provisioning for cash-out schemes.** Threat actors recognize that payment technologies like 3DS and digital wallets are effective, but they have also identified OTPs and inconsistent merchant onboarding as weaknesses to be exploited. This will likely continue to enable threat actors to adapt payment mechanisms for fraud rather than bypass them outright — especially when combined with time-tested social engineering tactics. Improving e-skimmer kits and new vulnerabilities will likely serve as major accelerants for e-skimmer-based fraud. Although the implementation of PCI DSS v.4.0's future-dated requirements will almost certainly change the Magecart threat landscape, the effectiveness of those requirements will likely be degraded by inadequate adoption among small- and mid-sized e-commerce merchants.
- **Dark web marketplaces will continue to serve as a centerpiece of the payment fraud ecosystem, with Telegram and similar platforms reserved for less experienced threat actors.** The fraud ecosystem is a semi-professionalized, global market involving suppliers who compromise data, buyers who purchase and monetize stolen data, and criminal online marketplaces connecting suppliers and buyers. Dark web sources offer advantages of scale, persistence, market security, and, crucially, anonymity — especially in light of Telegram's agreement to provide user data to authorities.
- **The explosion in check fraud seen in the US over the past three years will not recede, but financial institutions will be better equipped to drive down the ultimate check fraud losses.** There is no indication that check fraud will abate. Check fraud techniques devised during the distribution of stimulus checks during the COVID-19 pandemic are now widely available, and unlike many cyber-enabled fraud schemes, check fraud does not require substantial technical expertise. Nevertheless, financial institutions enter 2025 better equipped to reduce actual losses from check fraud. The major accelerants for financial institutions on this front will be the adoption of stolen bank check threat intelligence, organizational commitments to resource previously underequipped check fraud prevention assets, and driving business customers to adopt risk-reduction solutions such as positive pay.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

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 customers, 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 customers 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 1,800 businesses and government organizations across more than 75 countries to provide real-time, unbiased, and actionable intelligence.

Learn more at recordedfuture.com