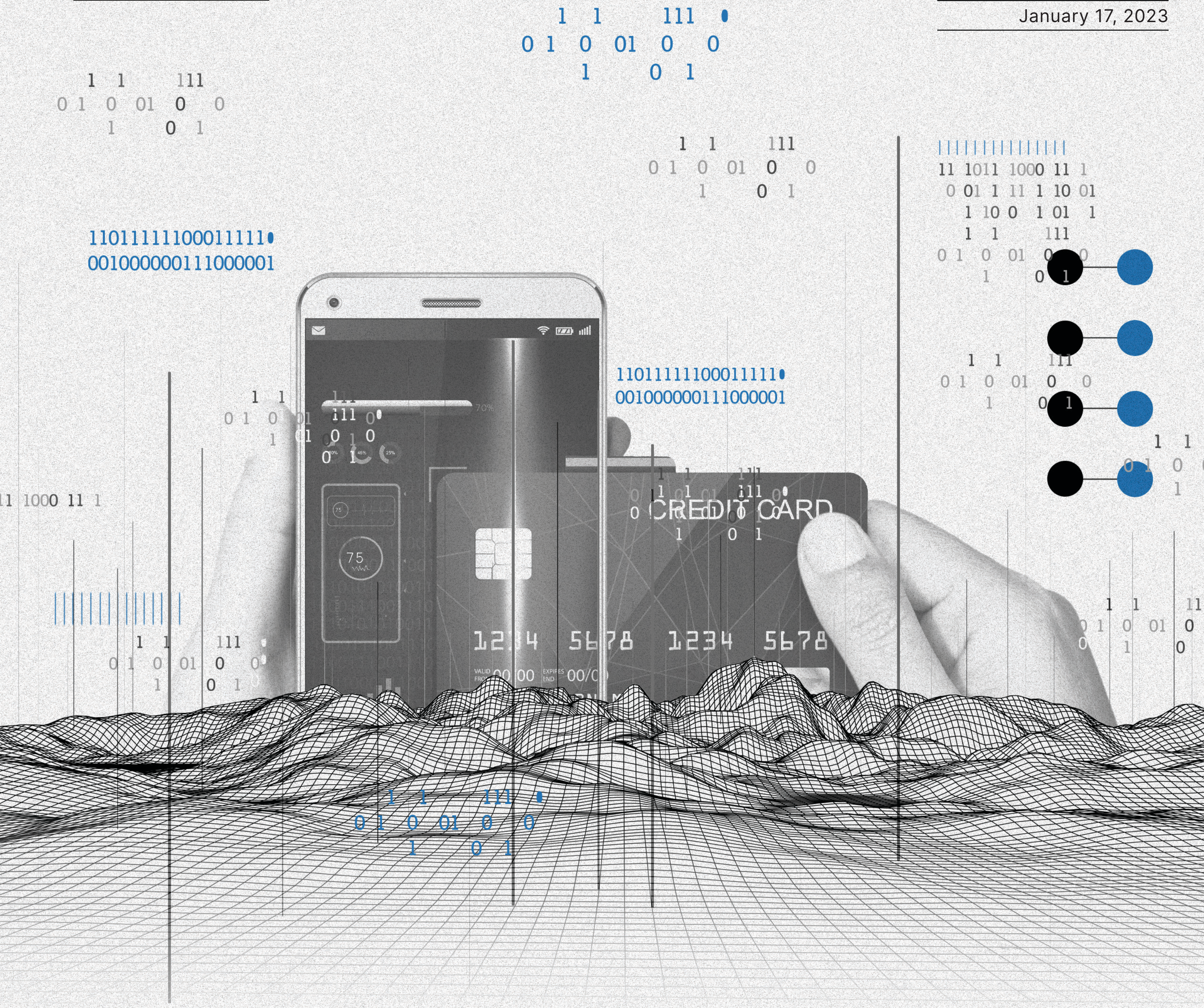
CYBER THREAT ANALYSIS

Recorded Future®

By Insikt Group®

January 17, 2023



Annual Payment Fraud Intelligence Report: 2022

This report provides trends and metrics for the payment card fraud landscape in 2022 and identifies the merchants most frequently compromised or abused as tester merchants. The target audience of this report is fraud and cyber threat intelligence (CTI) teams at financial institutions and merchant services companies.

Executive Summary

2022 was a year of system shocks, and the payment card fraud market did not survive unscathed. Russia's cybercrime crackdown — followed promptly by its full-scale invasion of Ukraine in February 2022 — spawned lower carding volumes for the remainder of the year. In total, 2022 saw 45.6 million card-not-present (CNP) and 13.8 million card-present (CP) payment card records posted for sale to carding shops on the dark web. These figures were considerably lower than the 60 million CNP and 36 million CP records posted for sale in 2021. Taken together, this decreased supply, demand, and turnover defined the payment card fraud market and threat landscape throughout 2022.

In spite of this, the card fraud market and the threat actors who populate it demonstrated remarkable resilience. Magecart actors launched campaigns that employed fake payment card forms, exploited legitimate merchant web infrastructure to deploy e-skimmers, and used HTTP referer headers to impede remediation by security analysts. One of these campaigns led to the compromise of 2 online ordering platforms, a trending tactic that exposes merchants who use the platforms to the risk of being compromised. Meanwhile, high-profile merchants were increasingly exploited by individual threat actors and checker services on the dark web in order to verify the validity of stolen cards. And finally, as war in Ukraine hampered cybercriminals' ability to engage in card fraud, one top-tier carding shop exploited the lull in supply by flooding the market with recycled payment card records. Although frustrated by these records' low quality, resourceful threat actors may nevertheless use them as cheap sources of personally identifiable information (PII) that they can weaponize to carry out targeted account takeover (ATO) attacks against their victims.

By employing proactive anti-fraud strategies that integrate intelligence from throughout the payment fraud life cycle, financial institutions and card issuers can reduce card fraud losses in 2023. The overall level of card fraud activity in 2023 will be highly dependent on whether or not Russia's war in Ukraine continues; if it does, threat actors' ability to engage in card fraud will likely remain degraded. But should the war end, a renewal or increase in payment card fraud may follow.

Key Findings

- 45.6 million CNP payment card records were posted across dark web carding shops in 2022, down 24% from 2021. It is highly likely that this year's relatively low CNP volumes are the result of Russia's early-2022 cybercrime crackdown and its subsequent full-scale invasion of Ukraine. In 2022, the highest-impact CNP breaches affected online ordering platforms.
- 13.8 million CP payment card records were posted across dark web carding shops in 2022, down 62% from 2021. While it is possible the year's events contributed to this drop-off, year-by-year CP volumes have also steadily declined due to the rising global adoption of more secure in-person payment methods. In 2022, CP breaches overwhelmingly affected small restaurants and bars.
- The Recorded Future® Magecart Overwatch program discovered 1,520 unique malicious domains involved in the infections of 9,290 unique e-commerce domains at any point in 2022.
- Full primary account numbers (PANs) for at least 20.5 million compromised payment cards were posted as plaintext or images to various resources including dark web forums, pastebins, and social media.
- 21 card checker services monitored by Recorded Future abused 2,953 unique merchants associated with 660 unique merchant identification numbers (MIDs) for illicit card checks.
- Threat actors focused on avoiding or bypassing protections offered by the 3-D Secure (3DS) protocol and increasingly discussed the abuse of customer service call centers as a means of facilitating their attacks. Furthermore, a surge in cheap, reposted payment card records posted throughout 2022 increased the attack surface for ATO attacks.
- The payment fraud life cycle closely resembles a real-world market underpinned by supply chains, coordinated exchange between buyers and sellers, and the provision of services such as checkers. Although this high degree of organization increases the opportunities and impact of card fraud, it also produces a data-rich environment. Therefore, card issuers, acquirers, and merchant service providers should incorporate and integrate intelligence from across the payment fraud life cycle to proactively combat fraud.

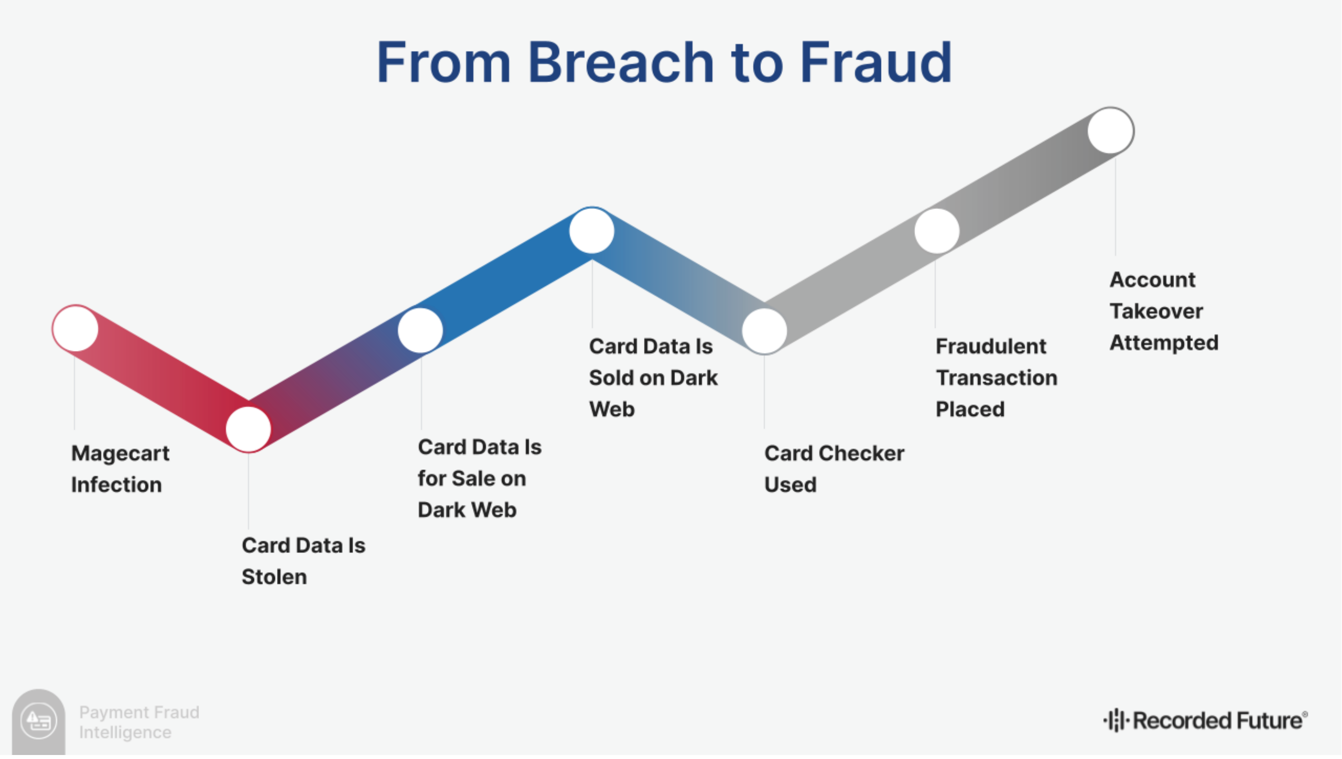

From Breach to Fraud
Magecart Infection
Card Data Is Stolen
Card Data Is for Sale on Dark Web
Card Data Is Sold on Dark Web
Card Checker Used
Fraudulent Transaction Placed
Account Takeover Attempted
Payment Fraud Intelligence
Recorded Future

Figure 1: *Payment card fraud conforms to a general life cycle (Source: Recorded Future)*

Background

Payment card fraud exists as part of a sophisticated underground economy. Production networks, supply chains, and dark web carding shops provide threat actors with the means to market criminal services and wares to their peers or to purvey stolen data to end users who engage in card fraud. Within this shadow economy, payment card fraud conforms to a certain "life cycle", as seen in Figure 1.

At the beginning of the life cycle, physical compromises facilitate the theft of payment card data from merchants' card-present (CP) transactions. Meanwhile, cybercriminals enact digital compromises — often with Magecart e-skimmer infections — to steal card data from online card-not-present (CNP) transactions. These stolen card records are posted for sale to the dark web, where partial payment card data is put on display so criminal buyers can go "window shopping". Occasionally, carding shops release full stolen payment card data for promotional purposes, which provides one of the many opportunities for criminals to snatch up full primary account numbers (PANs). Before making a sale, carding shops use aptly named checkers to appraise stolen card sets; individual criminals use the same checkers to verify their records' validity before or after purchase. Once "end user" fraudulent actors acquire their desired payment card data, they monetize it, usually through fraudulent transactions. If actors can acquire enough of a victim's personally identifiable information (PII), they can even attempt account takeover (ATO) attacks to cash out their victim's bank account.

Throughout 2022, Recorded Future monitored this shadow economy to empower clients to disrupt fraud at every stage of the payment card fraud life cycle. In the course of our monitoring, we observed both continuing trends from 2021 and novel trends that grew organically from the events of 2022.

Magecart E-Skimmer Infections

Magecart e-skimmer attacks are used to steal customer payment card data from e-commerce websites and exfiltrate it to the attackers' infrastructure. From there, stolen records can be sold on the dark web.

In 2022, Magecart attacks continued to enjoy popularity among dark web cybercriminal communities. Recorded Future observed 1,520 unique malicious domains that were used to host e-skimmer payloads or receive stolen payment card data from infected e-commerce domains. 9,290 unique e-commerce domains suffered from an infection at any point in 2022. Of these, 2,468 e-commerce domains remained actively infected at the close of 2022.

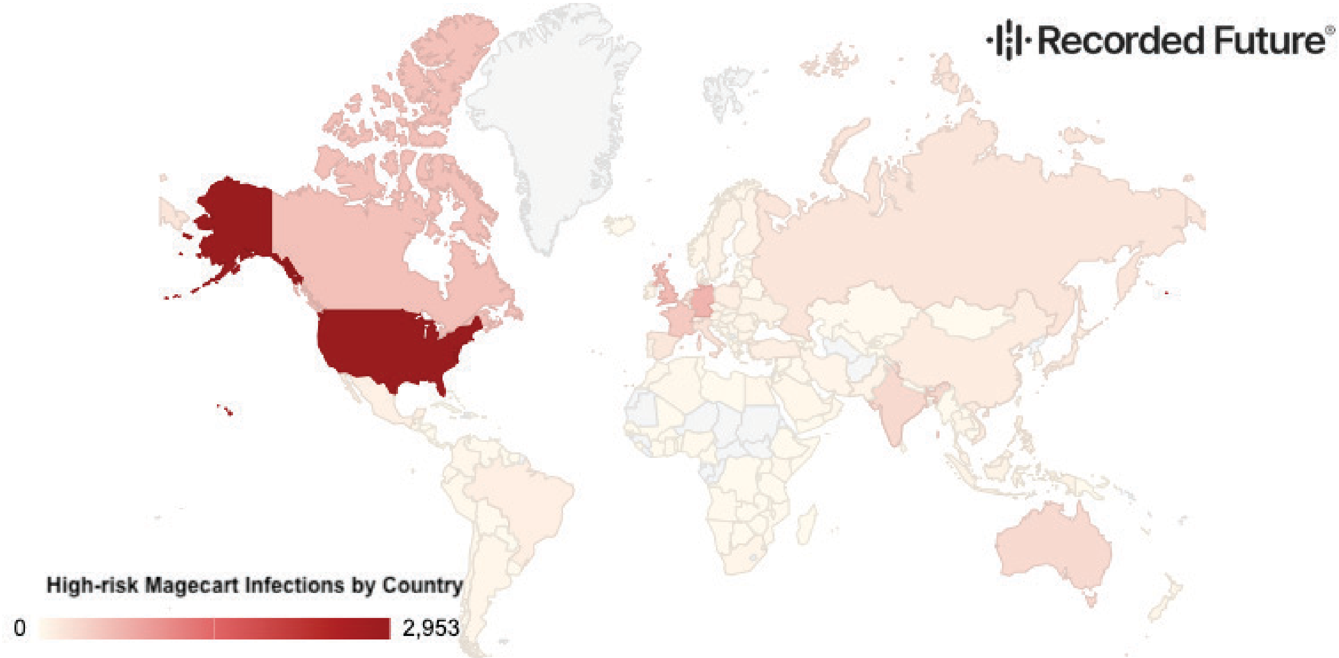


Figure 2: *Quantity of high-risk Magecart infections that affected each country in 2022 (Source: Recorded Future)*

Figure 2 shows the quantity of high-risk Magecart infections in each country. An infection is only considered high-risk for countries that appear in the infected website's "Top 5" sources of web traffic (according to Similar Web). If an infected website's web traffic data was unavailable, analysts substituted it with the location where the website was hosted to determine whether or not the infection was high-risk.

Fake payment card forms and attack-carrier domains (legitimate e-commerce domains that threat actors have compromised and incorporated into their attack infrastructure) enjoyed frequent use throughout 2022. In January 2022, Magecart Group 7 launched a Magecart campaign that saw fake payment card entry forms injected onto e-commerce websites to replace legitimate payment gateway subforms and inline frames (iframes). As previous attack-carrier domains became inaccessible, Magecart Group 7 repeatedly migrated its operations to new attack-carrier domains. In total, 12 attack-carrier domains were abused during this campaign to infect 1,141 websites.

Recorded Future also discovered a novel Magecart campaign in which a malware server used the HTTP referer header in requests to limit downloads of malicious scripts. Threat actors injected links to malicious JavaScript files into e-commerce shops, but the server hosting these files only sent the malicious scripts when: 1) HTTP referer headers were present; and 2) their value reflected the infected e-commerce websites. This technique was likely meant to impede security analysts in remediating infections. As with Magecart Group 7's campaign, this campaign's malware installed fake payment card forms on checkout pages.

In December 2021 and September 2022, we reported on how Magecart actors exploit Google Tag Manager (GTM) containers to infect e-commerce sites, and this trend continued throughout 2022. GTM is a legitimate web service used for internet marketing, website usage metrics, and customer tracking. 2 GTM-based e-skimmer variants have been involved in Magecart infections since as early as March and June 2021; a third was found in Magecart infections that began no later than July 2022. In total, we have detected 891 e-commerce domains that were infected by any of these variants.

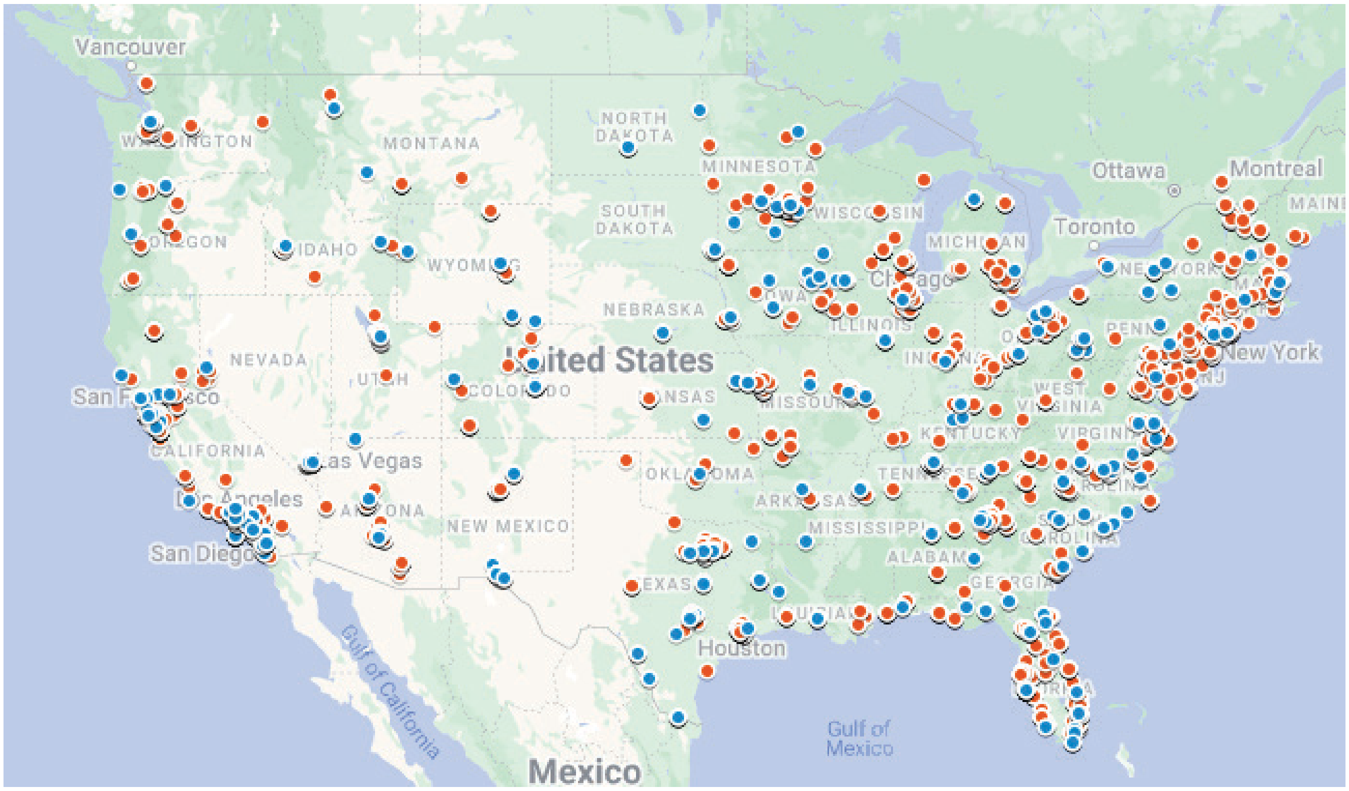


Figure 3: *Blue pins represent the physical location of merchants affected by CP breaches, whereas orange pins represent the headquarters for companies affected by CNP breaches (Source: Recorded Future)*

Top Payment Card Breaches in 2022

As we scour the web for Magecart infections, our analysts hunt down common points of purchase (CPPs) linked to stolen payment cards offered for sale on the dark web. Through collaboration with partner financial institutions, we reported breaches that exposed customer payment card data at over 1,000 unique merchants in 2022. For 77% of the merchants, we have identified compromised payment cards from the breaches on the dark web. As shown in Figure 3, merchants in all 50 states and the District of Columbia were affected, with the heaviest concentrations in major metropolitan areas.

While CP breaches overwhelmingly affected small restaurants and bars, CNP breaches predominantly affected e-commerce websites across various industries and were largely conducted through Magecart e-skimmer infections. The highest-impact CNP breaches occurred as a result of "platform breaches", which are attacks that compromise an e-commerce service that facilitates online sales or website management. By targeting an e-commerce service, threat actors create a disproportionately expanded attack surface, causing a significant number of client merchants that use the platform to be compromised.

Among this year's platform breaches, the highest-impact compromises targeted outsourced online ordering solutions for restaurants and ticketing solutions for entertainment and transportation companies:

- MenuDrive and Harbortouch, both of which are online ordering platforms for restaurants, were targeted by a single Magecart campaign that resulted in e-skimmer infections for 80 restaurants using MenuDrive and 74 using Harbortouch. This campaign began no later than January 18, 2022, and persisted into Q2 of 2022.
- Another online ordering platform, InTouchPOS, was targeted in a separate, unrelated Magecart campaign resulting in e-skimmer infections for 157 restaurants using the platform. This campaign began no later than November 12, 2021, and persisted into Q2 of 2022. Disturbingly, similarities in attack methodology suggest that the actors responsible for compromising InTouchPOS were also responsible for the HTTP referer header campaign (referenced in the Magecart section above).
- Core Cashless, an online ticketing platform for amusement parks, was breached, resulting in the exposure of payment card data from transactions at 45 amusement parks. First reported by Recorded Future in mid-July 2022, Core Cashless publicly acknowledged the breach in September 2022, claiming the breach lasted from January 2022 to July 2022.

Compromised Payment Cards on the Dark Web

Once threat actors have compromised payment cards, they can either attempt to fraudulently monetize the records themselves, or sell the compromised records to other actors, often via carding shops.

That said, the threat actors who compromise payment cards are rarely the same ones who use them to commit fraud. Payment card fraud is an unpredictable, time-consuming process. Fraudulent actors must operate logistical networks, resell goods and services, devise and execute cash-out schemes, and launder their criminal profits. Alternatively, threat actors can simply sell their stolen payment cards on carding shops to generate predictable, painless profits.

Magecart e-skimming is an illustrative example. In 2022, the average infected website saw 5,215 monthly visitors, and according to e-commerce platform BigCommerce, average customer conversion rates range from 2.5 to 3%. If threat actors collect between 130 to 160 cards per month from each of their infected websites and then sell them at an average price of $15 USD per compromised card, they could easily earn between $1,950 and $2,400 USD per month, per infected website. Magecart threat groups often operate dozens of e-skimmer infections at any given moment. This enables them to amass substantial criminal profits without sinking time and effort into fraudulent monetization.

Usually, threat actors who purchase compromised records are either: 1) "lower-tier" threat actors who lack the technical expertise to engage in widespread card collection; or 2) "mature" threat actors with established monetization and money-laundering networks. Carding shops serve as the connective tissue of the card fraud ecosystem, bringing together buyers and sellers.

Carding Shops and Trading Volumes

In 2022, 45.6 million CNP and 13.8 million CP payment card records were posted for sale across dozens of carding shops. Of these 59.4 million compromised payment card records, 70% were issued by financial institutions in the United States. The abuse of stolen CP records was once the dominant form of card fraud, but over the past few years the volume of CNP records posted for sale has overtaken CP records. 2 trends drive this shift:

- A decrease in CP volumes due to the rising adoption of secure in-person transaction technologies (such as EMV chips and contactless payment) and the massive reduction of in-person transactions during the COVID-19 pandemic
- An increase in CNP volumes due to Increased online shopping, the advancement of Magecart e-skimming techniques, and the proliferation of Magecart-as-a-service

This year, the card fraud market was heavily disrupted by geopolitically driven events. In January and February 2022, Russian law enforcement launched an unprecedented crackdown on domestic cybercrime, shutting down several top-tier carding shops. Given that the crackdown occurred during Russia's troop buildup on the Ukrainian border, the prevailing theory is that Russia sought to signal its intent to cooperate with the West against cybercrime should the West acquiesce to Russian demands regarding Ukraine.

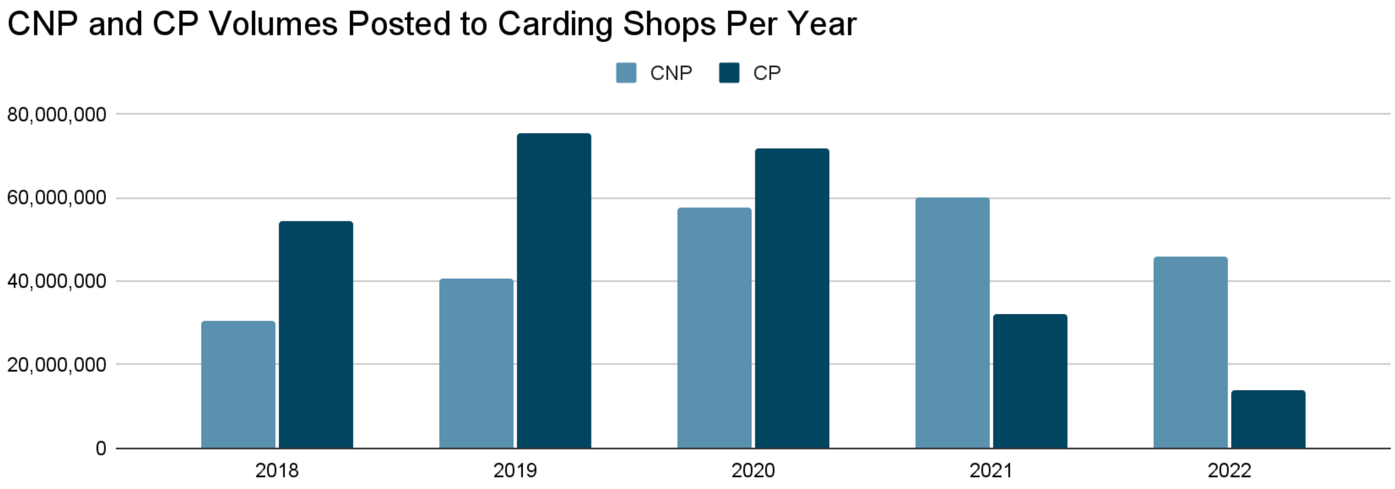


Figure 4: *In recent years, CNP records have overtaken CP records in both supply and demand (Source: Recorded Future)*

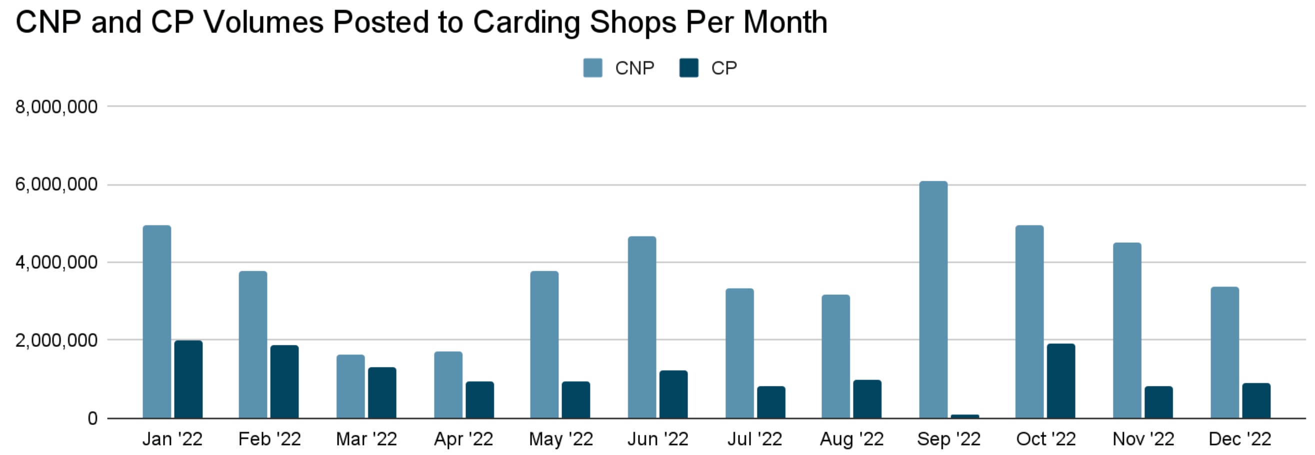


Figure 5: *Russian law enforcement's closure of carding shops in early 2022 severely decreased volumes in March and April 2022, before volumes began to rebound in May 2022 (Source: Recorded Future)*

Nevertheless, Russia invaded Ukraine in February 2022, quickly dispelling the climate of fear that had permeated the Russian dark web in the wake of the crackdown. The fear of prosecution by Russian law enforcement evaporated by mid-March 2022, and volumes rebounded as new carding shops assumed the lost market share. Yet by the second half of 2022, threat actors on card fraud-focused forums increasingly complained that compromised records were extremely "low quality" (no longer active and valid). At the same time, our internal analysis revealed that several large carding shops were flooding the market with low-priced, reposted, or fake records.

Ultimately, lower payment card volumes were posted in 2022 than 2021. From the second half of February through April, this was almost certainly a result of the Russian cybercrime crackdown. After April, lower carding demand and depressed volumes of "fresh" records were likely a result of Russia's war. It is highly likely that the war has significantly affected Russian and Ukrainian threat actors' ability to engage in card fraud as a result of troop mobilization, refugee and voluntary migration, energy instability, inconsistent internet connectivity, and deteriorated server infrastructure. (Russian-occupied areas of the Donbas region of Ukraine were long suspected to have hosted cybercriminal server infrastructure.)

Full Compromised Payment Card Data Posted to Forums, Social Media, and Other Resources

In addition to the 59.4 million partial payment card records posted to carding shops, the full primary account numbers (PANs) of over 20.5 million compromised payment cards were posted as plaintext or images across various resources including dark web forums, pastebins, and social media. Although posting the full, unredacted data of compromised card records deprives actors of potential profits from unrealized sales, a range of reasons exists for doing so. These include the following:

- Carding shops post compromised cards on fraud-focused forums and Telegram channels for marketing purposes
- Aspiring threat actors/groups post records on forums and Telegram channels to build their reputations
- Reckless or inexperienced threat actors post payment card records and images of compromised cards to social media
- Threat actors involved in negotiations post full records to "pastebins" as a quick and easy way to share data with other threat actors.

Together with the full PANs, threat actors also frequently post other associated card data (such as expiration date or CVV) and PII.

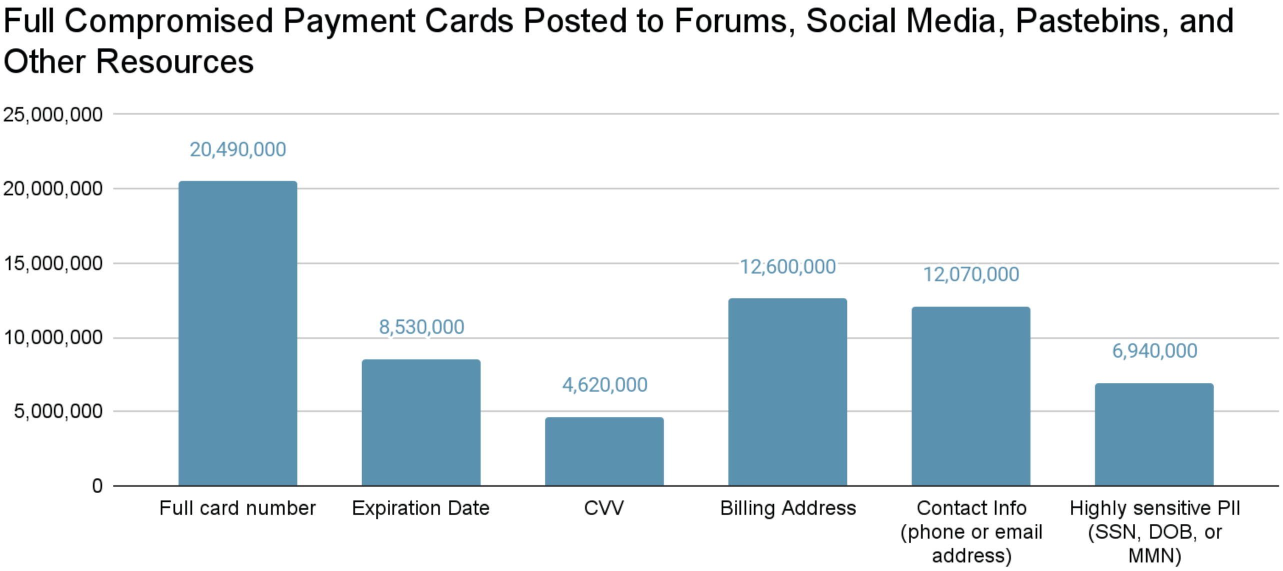


Figure 6: *In 2022, the full card numbers of 20.5 million compromised cards were either accidentally or intentionally posted to the web (Source: Recorded Future)*

"Checkers": Criminal Services for Verifying Compromised Card Validity

Often, purchasing stolen payment cards is the first step in a threat actor's efforts to make illicit purchases. Occasionally, the fraudster may purchase a card that has already been flagged as stolen by the issuing financial institution, barring the fraudster from monetizing that card. As a result, carding shops and individual fraudsters use "checkers": dark web services that allow them to determine if a card is valid or if it has been flagged as stolen.

Fraudsters access card checkers through dedicated checker services or dark web marketplaces that offer checker services through application programming interface (API) integration. To use the card checkers, fraudsters simply input the compromised payment card data and the checker performs automated checks. Card checkers verify card validity by either: 1) conducting a small CNP transaction, typically between $0.01 and $1.00; or 2) initiating a zero-dollar authorization request for the card, typically by linking the card to an account on an e-commerce or social media website. Checkers complete checks within seconds and inform the fraudster whether the card is valid (card accepted) or invalid (card declined).

Card-checking data provides financial institutions with a final warning signal before a compromised payment card is fraudulently monetized for a high-dollar transaction. By adding known "tester merchants" to a risk model, financial institutions can monitor their portfolio and raise the risk score for cards that conduct transactions or authorizations with known checker merchants.

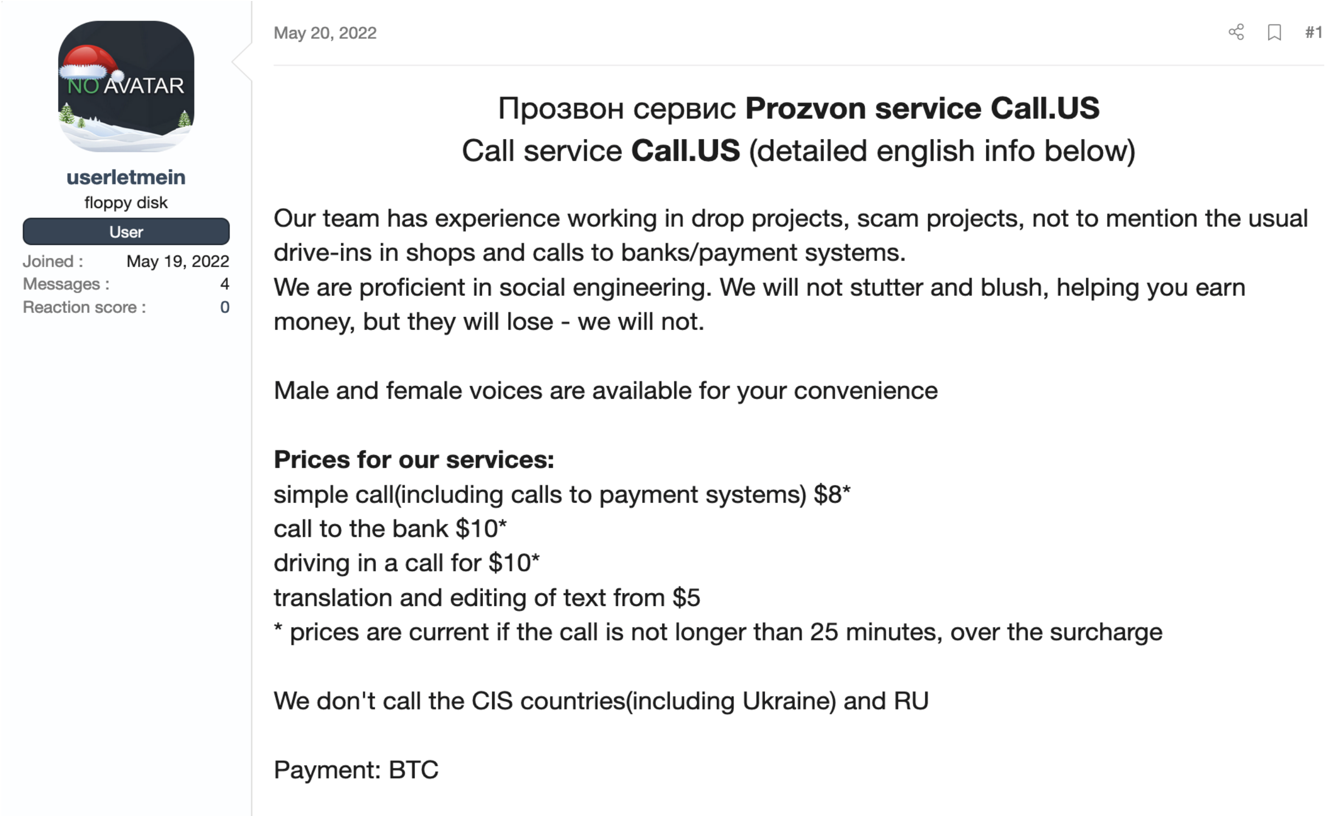
In 2022, 21 checker services monitored by Recorded Future abused 2,953 unique merchants associated with 660 unique merchant identification numbers (MIDs) for illicit card checks. Among the unique MIDs that surfaced during our checker services monitoring, the 5 most common merchant category codes (MCC) abused by checkers are listed below.

MCC	Description
8011	Doctors–not elsewhere classified
5999	Miscellaneous and Specialty Retail Stores
8099	Health Practitioners, Medical Services–Not Elsewhere Classified
7299	Other Services–Not Elsewhere Classified
8398	Organizations, Charitable and Social Service

Table 1: *The 5 most common MCCs based on the number of unique MIDs associated with each MCC (Source: Recorded Future)*

At the beginning of 2022, we predicted that donation sites would enjoy popularity for card checks because of their viability and discretion. This prediction appears to have held true: in 2022, MCC 8398 ("Organizations, Charitable and Social Service") ranked #5 among MCCs used for card-checking.

In 2022, one popular checker systematically incorporated high-profile merchants into its card-checking infrastructure, a strategy that is likely to enjoy wider adoption across other checker services and the threat actor community at large. Major merchants' web payment services present an effective and reliable means for checking stolen payment cards, and 4 of the top



Прозвон сервис **Prozvon service Call.US**
Call service **Call.US** (detailed english info below)

Our team has experience working in drop projects, scam projects, not to mention the usual drive-ins in shops and calls to banks/payment systems.
We are proficient in social engineering. We will not stutter and blush, helping you earn money, but they will lose - we will not.

Male and female voices are available for your convenience

Prices for our services:
simple call(including calls to payment systems) $8*
call to the bank $10*
driving in a call for $10*
translation and editing of text from $5
* prices are current if the call is not longer than 25 minutes, over the surcharge

We don't call the CIS countries(including Ukraine) and RU

Payment: BTC

Figure 7: *Responding to high demand in 2022, "userletmein" advertised their call support services (Source: XSS Forum)*

20 tester merchants this year were industry-leading companies in the news media, audio streaming, and transportation verticals. Similarly, threat actors discussing card-checking on dark web forums demonstrated interest in exploiting other high-profile merchants — including a market leader in activewear — for card checks. These companies have international client bases, and over the last 3 months they saw from 7.4 to 173.4 million monthly visitors to their websites. It is highly likely that threat actors are increasingly abusing high-profile merchants because these merchants:

- Process massive volumes of transactions and authorizations, making it more difficult for financial institutions to distinguish legitimate behavior from suspicious activity
- Operate internationally, allowing threat actors to more successfully check non-US cards

Fraudulent Monetization and Account Takeovers

Fraudsters focused great efforts on avoiding or bypassing 3-D Secure (3DS), which provides formidable security for online payment card transactions. To this end, 3 leading card-checker services added features in 2022 that allow fraudsters to check whether or not cards are 3DS-protected, likely in response to rising demand for non-3DS stolen payment cards.

For cases where cybercriminals had to bypass 3DS to monetize stolen payment cards, they increasingly turned to technical solutions. Historically, fraudsters have resorted to high-level social engineering techniques to bypass 3DS, but phishing panels are a recent technical innovation that facilitate phishing operations at scale, especially for threat actors who lack collection expertise. In 2022, a growing amount of phishing panels — including those capable of 3DS bypass — were developed for rent or sale as components in ready-to-go phishing packages. This is almost certainly part of a greater shift toward phishing-as-a-service (PhaaS) that has occurred in recent years.

Beginning in April 2022, a top-tier carding shop flooded the market with low-quality records that had previously been posted on a defunct top-tier carding shop. While these dated records were less actionable for monetization through payment card fraud, the availability of additional PII with these cheap records increased the attack surface for ATO attacks. 25% of email addresses listed with these low-quality records were available from other credential breaches across the web. By obtaining email addresses from these cheap, abundant records, and then cross-referencing them with other credential breaches, astute threat actors can likely locate additional victim PII. With this information in hand, they can refer to the bank identification numbers (BINs) from the cheap payment card records to enact targeted ATO attacks against their victims' bank accounts.

A related theme in fraudsters' TTPs this year was the growing abuse of call centers. Staff at call centers are trained to prioritize customer satisfaction, and threat actors have dialed in on this as a "weak link" in financial institutions' security posture. By contacting customer support centers and assuming the identities of their victims, fraudsters can leverage victim PII to verify available funds in their victims' accounts, withdraw or transfer funds, and confirm transactions. A multitude of dark web actors offer bespoke call services to facilitate these attacks, and although shrewd customer support representatives frequently detect and prevent fraud, threat actors can compensate for failed attacks through volume. For fraudsters, one successful social engineering call can justify dozens of fruitless attempts.

Mitigation

Financial institutions that may be exposed to payment card fraud losses from both their card-issuing and card-acquiring functions should incorporate and act on intelligence from each stage of the fraud life cycle to mitigate the financial and reputational costs of payment fraud. The payment fraud ecosystem closely resembles a real-world market. Although this sophistication increases the threats and costs that the payment fraud ecosystem imposes on the entities it affects, it also serves as a rich source for valuable intelligence.

Financial institutions should also employ a proactive anti-fraud approach that establishes e-skimmer intelligence as a foundational pillar of transaction monitoring, risk scoring, and reissuance rules. Historically, card issuers have primarily relied on "reactive" common point of purchase analysis to trace fraudulent transactions conducted with payment cards back to the source of compromise.

Card issuers should also leverage carding shop intelligence to identify compromised payment cards within their portfolio that are being sold on the dark web. The majority of compromised payment cards that eventually turn into fraudulent transactions first appear on carding shops.

Finally, card issuers should systematically incorporate checker intelligence into risk-scoring processes in order to surface compromised payment cards that have otherwise remained undetected. Threat actors turn to checkers to verify the validity of compromised payment cards later in the payment fraud life cycle. These card checks provide card issuers with a vital final signal before high-dollar fraudulent transactions are attempted.

Outlook

The Nilson Report recently reported that in 2021, "card issuers, merchants, acquirers of card payments from merchants, in addition to acquirers of card transactions from ATMs incurred gross fraud losses of $32.34 billion, up 13.8% from 2020". In 2022, however, depressed trading volumes seen on carding shops diminish the likelihood that payment card fraud losses last year underwent an equally large increase.

In any market economy, players live and die by the rule of "survival of the fittest" — and the card fraud market is no exception. But if the events of 2022 had a chilling effect on the payment card fraud market and threat landscape, the resulting volumes and turnover are far from a death knell. On the contrary, the austere economic conditions that occurred this year demonstrate that the card fraud underground is fully capable of evolving to survive systemic shocks.

For 2023, we assess that the future of the card fraud market will remain highly dependent on external events. Should Russia's war in Ukraine continue, the factors influencing regional threat actors' ability to engage in card fraud will likely persist, and threat actors' ability to engage in card fraud will remain lower than before the war, even as they continue to adapt. If the war should end, monitoring the region's post-war economies will be crucial to determine whether the conditions and incentives exist for a renewal — or possibly even an increase — in card fraud activity.

About Insikt Group®

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

About Recorded Future®

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

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