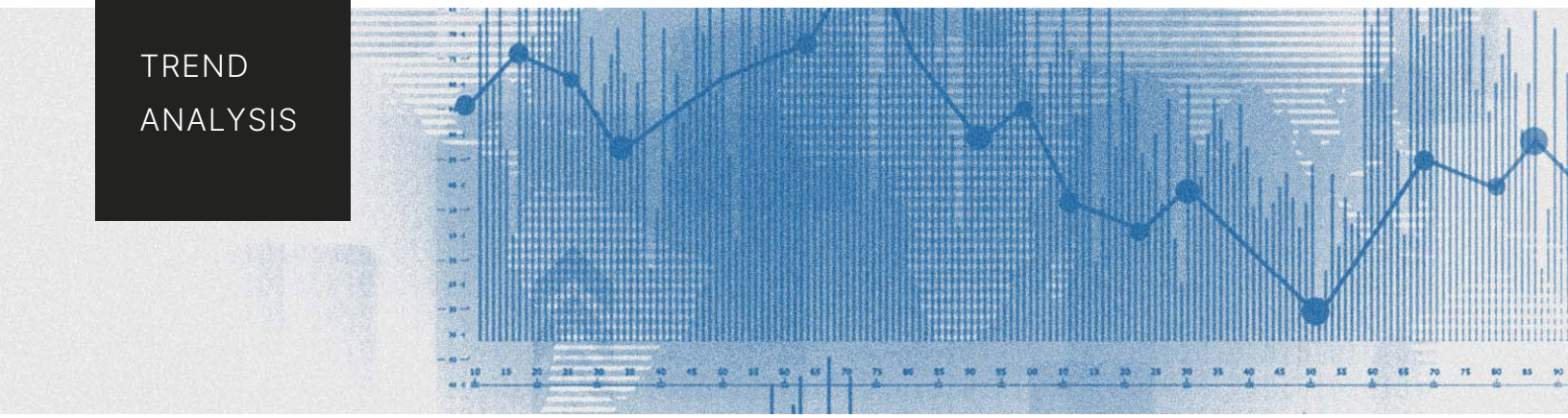
TREND ANALYSIS



CARD FRAUD REPORT 2021:
Magecart Thrives in the Payment Card Fraud Landscape

Key Findings

- The underground payment card economy in 2021 saw new tactics enable new attack vectors, raising certain fraud schemes to higher prominence, such as attacks leveraging Google Tag Manager (GTM) and WebSockets, the Skimmer-as-a-Service model, and card checker innovations.
- The levels of Card Present (CP) records offered for sale on the dark web have continued to decline, furthering the trend that COVID-19 accelerated away from CP cards and towards Card Not Present (CNP) records.
- Cybercriminals have demonstrated the efficiency of compromising multiple merchants with a single attack by targeting ordering platforms that service dozens of merchants.
- Gemini Advisory, a Recorded Future® company, assesses with high confidence that the shift towards CNP is likely here to stay (albeit potentially less extreme in post-COVID conditions) and that Magecart attacks will likely remain dominant in the near future.

Background

The underground payment card economy in 2021 maintained the previous year's trends as it continues to emerge from the COVID-19 pandemic conditions. However, new tactics have enabled new attack vectors, raising certain fraud schemes to higher prominence. Gemini Advisory's dark web intelligence offers insight into the most notable trends in 2021's fraud threat landscape.

The levels of Card Present (CP) records offered for sale on the dark web have continued to decline, furthering the trend that COVID-19 accelerated away from CP cards and towards Card Not Present (CNP) records. While there were over 70 million CP cards for sale in 2020, only 36 million appeared in 2021. Conversely, there were 40 million CNP records for sale in 2020 and 60 million in 2021, demonstrating relative consistency. The United States remained far and away the most common source of compromised payment card records.

Alongside the growing proportion of dark web CNP carding fraud has come a steady slew of Magecart attacks. These also primarily target the United States but have used increasingly sophisticated tactics, including Telegram bots, scripts that transmit payment card skimmer scripts and stolen data over WebSocket connections, and scripts that abuse Google Tag Manager (GTM) containers to conceal malicious scripts. Malicious actors particularly targeted small to medium-sized merchants that often lack the security resources of larger companies. Additionally, attacks on third-party payment processors offered actors a unique opportunity wherein a single compromise provides access to capture card data from the transactions of dozens of companies. Another emerging trend is the Skimmer-as-a-Service model, which lowers barriers-to-entry by providing the card skimming and data sales components allowing cybercriminals to focus on the identification and exploitation of vulnerable e-commerce sites.

In-Depth Analysis

Magecart

Magecart attacks have become increasingly popular among dark web cybercriminal communities. They allow hackers to skim customer card data from e-commerce sites' checkout pages and exfiltrate them to the attackers' infrastructure, from which they can sell the payment card records on the dark web. Online transactions became even more salient during the COVID-19 pandemic, raising the profitability of Magecart attacks.

Gemini Advisory has discovered over 1,132 unique attacker domains responsible for hosting malicious payloads or receiving stolen payment cards this year. Furthermore, analysts found thousands of unique attacker scripts, which indicates numerous variations among these attacks and complicates identifying them. Unique attacker domains have nearly doubled compared to last year's levels, while unique attacker scripts have increased 20-fold. As attacks become more lucrative, cybercriminal infrastructure has likewise grown.

The most common country from which hackers launched Magecart attacks in 2021 was the United States, followed distantly by Russia and then Germany. This is a sharp reversal from last year when Russia led and the United States closely followed it, with Germany far behind. This reflects the shift to the mega internet service and cloud hosting providers such as Amazon Web Services, Microsoft Azure, and Google Cloud Services. Fraudsters abuse these providers for their criminal schemes to appear more legitimate by hosting their malicious payloads in the United States.

Of the Magecart infections active in 2021:

- 2% saw a single infection while 18% showed indicators of multiple infections.
- 27% of sites with multiple infections were re-infected after removal of the prior infection, indicating the means of access was likely left unrepaired
- 73% of sites with multiple infections experienced overlapping infection windows, sometimes as a result of the original actor transitioning to new infrastructure.
- 171 days is the average length of infection.

Magento remained the most common e-commerce platform targeted by Magecart attacks. Given that Magecart attacks were originally named for Magento, this is consistent with past trends. OpenCart was the next-most targeted platform, followed by WooCommerce. Because the above platforms are typically hosted on a server acquired and maintained by the e-commerce merchant, they often fall behind in the installation of platform security patches, leaving known vulnerabilities available for exploitation by malicious actors.

One widely used and disturbingly effective technique was the infection of sites with trojanized GTM containers. Attackers placed their e-skimmer scripts within a GTM container because many security scanners overlook elements from "trusted" domains, thus allowing them to leverage a legitimate service for nefarious activities. Gemini Advisory has discovered 2 different Magecart GTM techniques that hackers have used to obtain more than 88,000 payment cards to offer on the dark web. Both techniques are effective and tend to evade automated scanners and security researchers, offering hackers the ability to establish and maintain persistence on the victim e-commerce sites.

To compound the danger from Magecart attacks, the Skimmer-as-a-Service model has grown more common among dark web communities. Similar to Ransomware-as-a-Service (RaaS), this offering allows less technical cybercriminals to hire expert hackers to write malicious scripts, embed card skimmers on their compromised sites, or even launch attacks on their behalf. It represents an increasing specialization and commercialization of cybercrime in which individuals focus their energy toward specific tasks and work for one another in order to launch the most effective attacks against even robust defenses. The RaaS model proved extremely prolific and correlated with a spike in ransomware attacks; the Skimmer-as-a-Service model may well follow suit.

Supply and Demand

In 2021, the yearly supply of compromised CP records in dark web marketplaces decreased by 49% to 36 million, marking the second consecutive yearly drop (2020 experienced a 10% drop to 70 million) after posting 50% year-over-year (YoY) growth in 2018 and 25% in 2019. Furthermore, demand for CP records dramatically declined again by roughly 50%. The ongoing COVID-19 pandemic and lockdown restrictions continued to drive down both the availability and demand for CP records as online shopping remains the dominant purchasing method.

Since 2017, the yearly supply of compromised CNP records in dark web marketplaces has continued to grow at a consecutively smaller rate of increase, resulting in 60 million cards exposed in 2021 which is a 9% increase from 2020's 55 million. Demand for CNP records increased by 16% in 2021. Whereas the data strongly suggests that the COVID-19 pandemic continued to cause a drop in demand for CP records, the data does not indicate a strong relationship between the ongoing pandemic and demand for CNP records.

For the fourth year in a row, the United States was the largest issuer country of compromised payment cards; nearly 90% of exposed CP cards and 59% of exposed CNP cards added to the dark web were issued by US card issuers. The consistently high percentage of exposed CP cards is due to the continued prominence of magnetic stripe transactions due to the slower adoption of EMV-enabled point-of-sale (POS) devices from merchants in the United States as compared to those of other developed countries. These attacks continually target small businesses; these merchants often have limited resources to devote to securing their systems and are thus more likely to remain infected for a longer period of time. For the third consecutive year, the second-highest issuer of compromised CP cards was South Korea. It is important to note that while South Korea remains one of the more-targeted countries for CP breaches, a large part of its compromised card volume comes from single events rather than a high baseline rate of breaches; this has been true in past years as well. The second-highest issuer of exposed CNP cards was Australia, unlike the previous year.

CPP Overview & Significant Breaches

While Gemini Advisory scours the web for Magecart infections, analysts also distinctly search for breaches linked to stolen payment cards offered for sale on the dark web. In 2021, Gemini Advisory identified new breaches of 1,590 merchants located across 48 states and 10 countries/territories in this way. Analysts mapped the US locations, which constituted the majority of data points, to indicate which regions, states, and cities were most heavily affected. Blue points represent CP breaches and refer to the physical location of the breached merchant. Orange points represent CNP breaches and refer to the physical headquarters of the company operating the website that was breached.

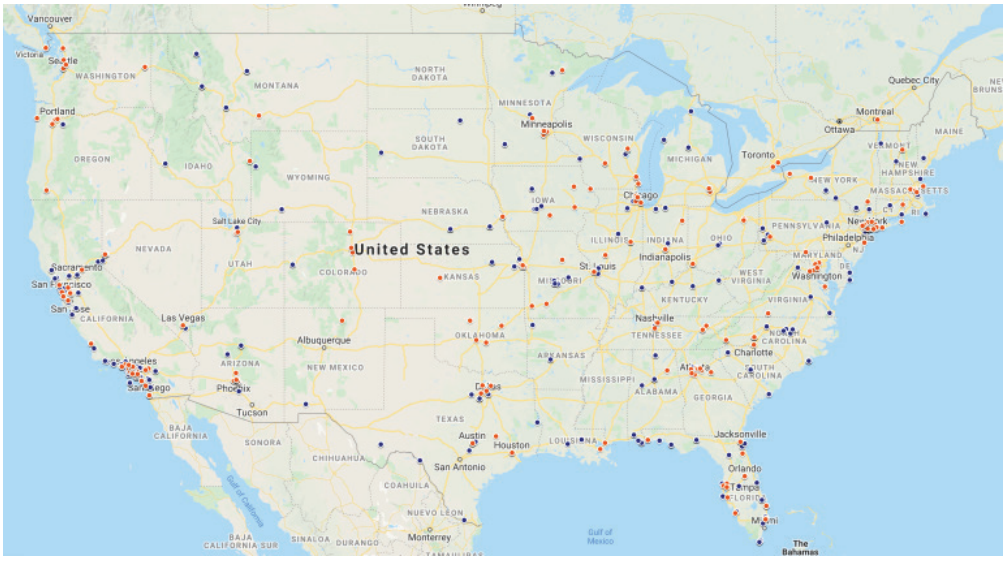


Image 1: The affected CPP locations are spread across the continental United States with a particular concentration in urban coastal regions. Blue points represent CP locations and orange points represent CNP locations.

Several of the most notable breaches this year are as follows:

- January: Gemini Advisory identified over 56,000 compromised records from 30 merchants using the Easy Ordering online ordering platform, which is owned by the Chicago-based restaurant technology company McPOS. The affected restaurants use EasyOrdering URLs through their respective websites.
- April and May: Over 18,000 records were posted to the dark web from two PoFolks locations in Enterprise, Alabama and Pensacola, Florida. PoFolks is a small chain of American homestyle cooking restaurants with six locations in Florida and one in Enterprise, Alabama.
- May: Nearly 20,000 compromised records were stolen from Oquossoc Grocery, a full service grocery market in downtown Oquossoc, a village of Rangeley, Maine. Analysts determined that the majority of records were compromised during EMV chip card transactions, indicating a more sophisticated level of malware was installed on the merchant's systems.
- June: Records appeared on the dark web from The Montana Club, a chain of American steakhouse restaurants with locations in Billings, Butte, Great Falls, Kalispell, and Missoula, Montana. This merchant's exposure dates back to March 2020 and has now seen over 100,000 compromised records posted to the dark web from multiple breaches.
- July: Cybercriminals posted over 110,000 compromised records to the dark web from over 268 merchants using PetExec as their payment and customer reservation processor. PetExec is a cloud-based system that provides various services, including payment processing, to pet care companies and was breached from July 1, 2020 to June 30, 2021.
- August: Cybercriminals posted 13,000 compromised records to the dark web from Film Alley, a regional chain of movie theaters with three locations throughout Texas, and is a subsidiary of Schulman Theaters. The records released indicated a breach of a specific Film Alley location in Weatherford, Texas.
- August: Over 8,000 records were posted to the dark web from Eli's Essentials, a wine bar in the Upper East Side of New York, belonging to the Eli Zabar line of businesses. Gemini Advisory reported two sets of records from the breach at Eli Zabar's E.A.T. catering business on July 30, 2020 and October 15, 2020. The malicious actors behind these attacks likely moved laterally through the Eli Zabar corporate network and installed skimmers on multiple POS systems.
- November: Gemini Advisory found more than 438,000 compromised records posted to the dark web that were linked to Running Warehouse, Tennis Warehouse, and Tackle Warehouse. These three merchants belong to Sports Warehouse, which has one headquarters in San Luis Obispo, California, and another in Alpharetta, Georgia.

Dark Web Disruption

Joker's Stash, the largest dark web marketplace in the underground payment card economy, announced its shut down in a post made January 15, 2021. The site's administrator, "JokerStash", claimed that the shop would remain operational until February 15, 2021, before the administrator "goes on a well-deserved retirement."

Joker's Stash was one of the oldest observed dark web marketplaces and has operated since 2014. In 2020, the marketplace has added over 40 million new records, the majority of which were CP. The CP data was linked to major breaches and the bulk of the CNP data was linked to Magecart attacks, although analysts also observed data obtained through phishing attacks. Gemini Advisory calculated that Joker's Stash has generated more than $1 billion USD in revenue over the last several years. After this marketplace went offline, its vendors and buyers transitioned to other top-tier dark web shops to continue with their illicit commercial endeavors. AllWorld, another dark web marketplace, is attempting to position itself as the replacement for Joker's Stash. It first emerged in May 2021 and gained notoriety by posting 1 million compromised payment cards for free. While Joker's Stash never posted free cards, it was known for large postings, so this may be part of AllWorld's strategy to replace it.

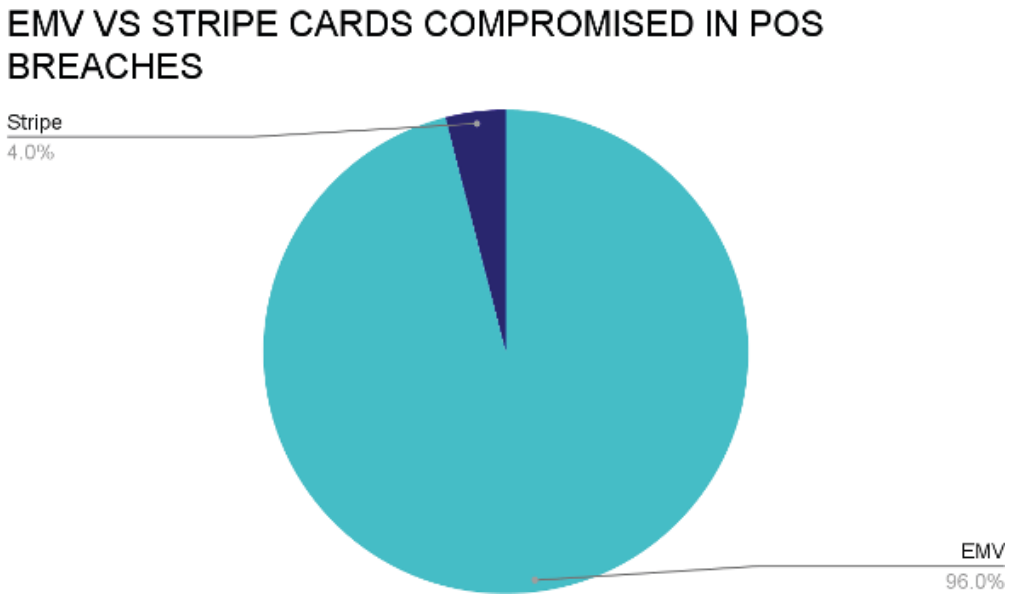


Image 2: The overwhelming majority of CP records compromised from POS systems were EMV-enabled.

Card Present (CP) Exposure

From the 462 CP breaches that Gemini Advisory reported on and analyzed in-depth, analysts determined that the average exposure window for CP breaches was 132 days, and that the majority of CP exposures in 2021 continued to come from restaurants and bars (MCC: 5812-5814). These establishments have been the primary target of CP breaches for the past several years because they continue to use outdated POS systems that only accept swipe transactions, a less secure payment method than EMV chip-enabled transactions. Restaurants and bars are also vulnerable to pocket skimmers, which can be used by malicious wait staff to surreptitiously collect the magnetic stripe data while the card is out of view.

Gemini Advisory has also observed cybercriminals targeting groups of merchants that use a common payment processor system for all of their transactions. For example, analysts found 48 different CP breaches, most of which are Thai restaurants, that used a payment processor that is no longer in service as of this writing. This gives them the advantage of compromising multiple merchants through a single breach.

Card Not Present (CNP) Exposure

Gemini Advisory analyzed in-depth and reported on 1,145 CNP breaches in 2021 and observed that threat actors relied on both established methods, such as Magecart-based attacks, as well as turning to increasingly sophisticated phishing attacks. On average, US victims' e-commerce sites that were targeted by a CNP-based breach remained infected for 188 days, while non-US victims' sites were infected for 171 days. Online retailers and merchants that offer e-commerce services continue to be targeted; in 2021, industries ranged from clothing, home decor, and industrial/automotive parts and components.

Furthermore, cybercriminals continued to target the websites of restaurants offering online ordering due to COVID-19's impact on indoor dining. This particularly impacted third-party payment portals for multiple merchants; breaching such a portal allows a single point of compromise to expose potentially dozens of participating companies. Gemini Advisory has noted breaches of four online ordering platforms servicing small restaurants that exposed 343,000 customer payment cards altogether.

Card Checkers

Often, purchasing stolen payment cards from the dark web is just the first step in a fraudster's efforts to make illicit purchases. In some cases, the fraudster may have purchased a card that has already been flagged as stolen by the issuing financial institution, barring the fraudster from placing illicit purchases with that card. As a result, dark web marketplaces and individual fraudsters often use "card checkers", which are dark web services that allow fraudsters to test whether a card is valid for conducting fraudulent activity or has already been flagged as stolen.

Fraudsters access card checkers through dedicated checker sites or dark web marketplaces that offer checker services through Application Programming Interface (API) integration. To use them, fraudsters simply input the compromised payment card data, and the checker automates the rest. Card checkers verify a card's validity by either conducting a small CNP transaction (typically between $0.01 and $1.00) or linking the card to an account on an e-commerce or social media website, resulting in a zero dollar authorization. Checkers typically complete checks within seconds and inform the fraudster whether the card is valid (card accepted) or invalid (card declined).

Gemini Advisory has observed several trends throughout 2021 with regards to the ways in which checker services operate. In September 2021, Gemini Advisory reported on a method in which cybercriminals use nonprofit organizations that accept donations to test a stolen card's validity. The challenges that donation sites pose to financial institutions attempting to monitor card testing activity makes these sites particularly appealing to cybercriminals. Given the viability and discretion of donation sites for card testing, they are likely to remain popular in dark web carding communities.

One of the most prominent card checking services has even added a feature allowing fraudsters to choose the type of merchant used to test stolen cards. Based on data collected by Gemini Advisory on various checker services, the top five Merchant Category Codes (MCC) used by the checkers in 2021 were the following:

MCC	Description
599	Miscellaneous and Specialty Retail Stores
8011	Doctors– Not Elsewhere Classified
5074	Plumbing and Heating Equipment and Supplies
7299	Donations / Personal Use
5941	Sporting Goods Stores

Gemini Advisory also observed that some checkers rotate through a variety of merchants frequently, while others utilize the same merchant for a longer period of time before changing to another. This level of complexity increases the difficulty for financial institutions to detect such activity.

Emerging Trends

The 3D Secure (3DS) security protocol provides an extra security layer for online credit and debit card transactions, allowing payment authentication to take the form of a fingerprint or facial recognition rather than only passwords or confirmation text messages. Despite its overall effectiveness, Gemini Advisory has observed dark web forum discussions focused on bypassing 3DS. They discussed tactics such as various social engineering techniques and phishing or scam pages. These can include tricking the victim into revealing their passwords by leveraging already-exposed personally identifiable information (PII) and impersonating a bank representative, often with the help of spoofed phone numbers. Malware and technical attacks, however, are not as effective against 3DS version 2.0.

The European Union's 3DS mandates lead global implementation, although levels vary worldwide. More widespread 3DS implementation will improve online transaction security, even if it can be bypassed with the right tools, effort, and skill set. While it is an upgrade to the security of many current online transactions, adopters must remain vigilant for determined attackers capable of executing high-level social engineering schemes.

Gemini Advisory has also observed a new wave of phishing attacks in the year 2021. This follows an increase in phishing volume in 2020, including a 72% increase in the number of dark web forum posts that mention phishing; this trend of increased phishing mentions continued in 2021. Cybercriminals are now designing phishing pages targeting customers of small and mid-sized banks, a tactic previously considered less lucrative than those targeting large financial institutions. However, these smaller banks often have fewer resources to dedicate to cybersecurity. This model is very compatible with phishing-as-a-service (PhaaS), a model in which skilled cybercriminals design phishing pages and sell them to less skilled criminal actors, who then launch their own campaigns.

Clever fraudsters also buy compromised payment card records or compromised bank login data that cannot be used for conventional fraud. For example, the cards may have expired or compromised bank login data (files with user login credentials, cookies, PII, etc.) become obsolete after the user changes their password. They do, however, usually contain the victim's email address or phone number, which a skilled phisher can leverage to convincingly mimic a legitimate message from the bank. Incomplete sets of PII are also useful in this capacity. Fraudsters increasingly launch either semi-targeted or spear phishing campaigns, the success of which lends further credibility to the PhaaS model.

Conclusion

The year 2021 was largely a continuation of the drastic developments of 2020. The shift away from CP fraud and towards CNP fraud extended during the second year of the COVID-19 pandemic. The United States remained the most targeted nation for fraud, Magecart continued to rise, and new CNP innovations dominated the threat landscape. Particularly savvy Magecart tactics, such as attacks leveraging GTM and WebSockets, proved effective, and the Skimmer-as-a-Service model consistently demonstrated promise. Gemini Advisory assesses with high confidence that the shift towards CNP is likely here to stay (albeit potentially less extreme in post-COVID conditions) and that Magecart attacks will likely remain dominant in the near future.

About Recorded Future

Recorded Future is the world's largest provider of intelligence for enterprise security. By combining persistent and pervasive automated data collection and analytics with human analysis, Recorded Future delivers intelligence that is timely, accurate, and actionable. In a world of ever-increasing chaos and uncertainty, Recorded Future empowers organizations with the visibility they need to identify and detect threats faster; take proactive action to disrupt adversaries; and protect their people, systems, and assets, so business can be conducted with confidence. Recorded Future is trusted by more than 1,000 businesses and government organizations around the world.

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