cybersixgill

REPORT

UNDERGROUND FINANCIAL FRAUD H1 2022

JULY 25, 2022

Contents

Executive Summary

- During the first six months of 2022 (H1 2022), 4,562,998 compromised payment cards were advertised for sale on underground credit card markets monitored by Cybersixgill. This marks a ~67.8% decrease from the total number of cards detected for sale on the deep and dark web in H2 2021 (14,185,859).

- Two underground credit card markets dominated 53% of the total market share as evaluated according to Cybersixgill's sources, while previously prominent markets were shut down.

- Compromised cards issued in the United States constituted approximately 45% of the global market share of cards sold on illicit credit card markets. This continued dominance of US-originating cards indicates the persistence of existing trends, whereby American cardholders remain the primary victims of financial fraud in underground markets.

- The United States maintains its number one spot in the global market share of compromised credit cards, while those originating from Russia rank closer to the bottom of the list. This indicates that many of the threat actors involved in credit card fraud are likely based in Russia, where they are free to act with impunity, as long as they do not defraud Russian targets.

- Compromised credit cards sold on the underground during H1 were primarily issued by the four major payment networks: 48.4% of the compromised credentials were issued by Visa; 35.8% by Mastercard; 12.9% by American Express; and 2.5% by Discover.

- Cards sold with CVV/CVV2 information were far more prevalent than those sold as dumps, at a ratio of 75% to 25%. This is entirely congruent with previously identified trends, providing further evidence to support the assumed preference of threat actors for CVV/CVV2 cards and the reduced risk of exposure of "card-not-present" fraudulent purchases.

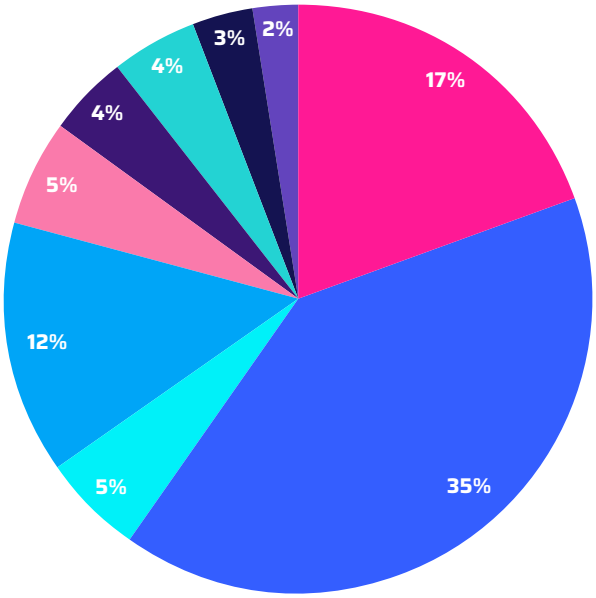
Introduction

Financial data is a valuable commodity on the digital underground, with payment card information constituting one of the more common items listed for sale. Threat actors typically obtain this information by targeting e-commerce sites through data breaches and phishing scams, or with physical hacking tools such as skimmers and shimmers installed on ATMs, point-of-sale terminals, and gas stations. Once in possession of stolen payment card data, threat actors work to monetize the information by selling it on underground credit card markets, where it is purchased by those who want to use them for various fraudulent activities.

Given the importance of stolen payment cards within the cybercriminal ecosystem, this report will examine the incidents of financial fraud that took place on the deep and dark web during the first six months of 2022 (H1 2022). During this period, 4,562,998 compromised cards were offered for sale on underground credit card markets monitored by Cybersixgill. This marks a dramatic decrease in cards offered for sale compared to H2 2021 (14,188,709) – a decrease of approximately 67%.

Analysis by credit card market

Although the underground is replete with credit card markets offering stolen payment cards for sale, in the first half of 2022, two underground shops accounted for approximately 53% of the total market share.

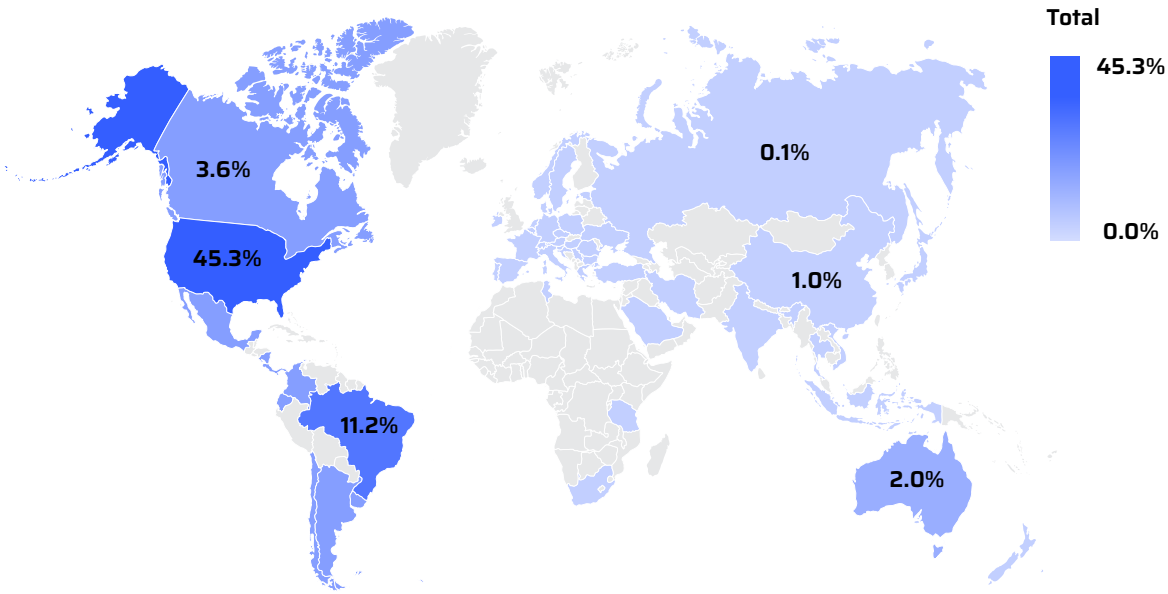


Segmentation of compromised cards sold on the underground in H1 2022 per market

The largest marketplace listed a total of 1,618,758 cards in H1 2022.

Segmentation of compromised cards sold on the underground in H1 2022 per market

Geographic Distribution of Compromised Cards

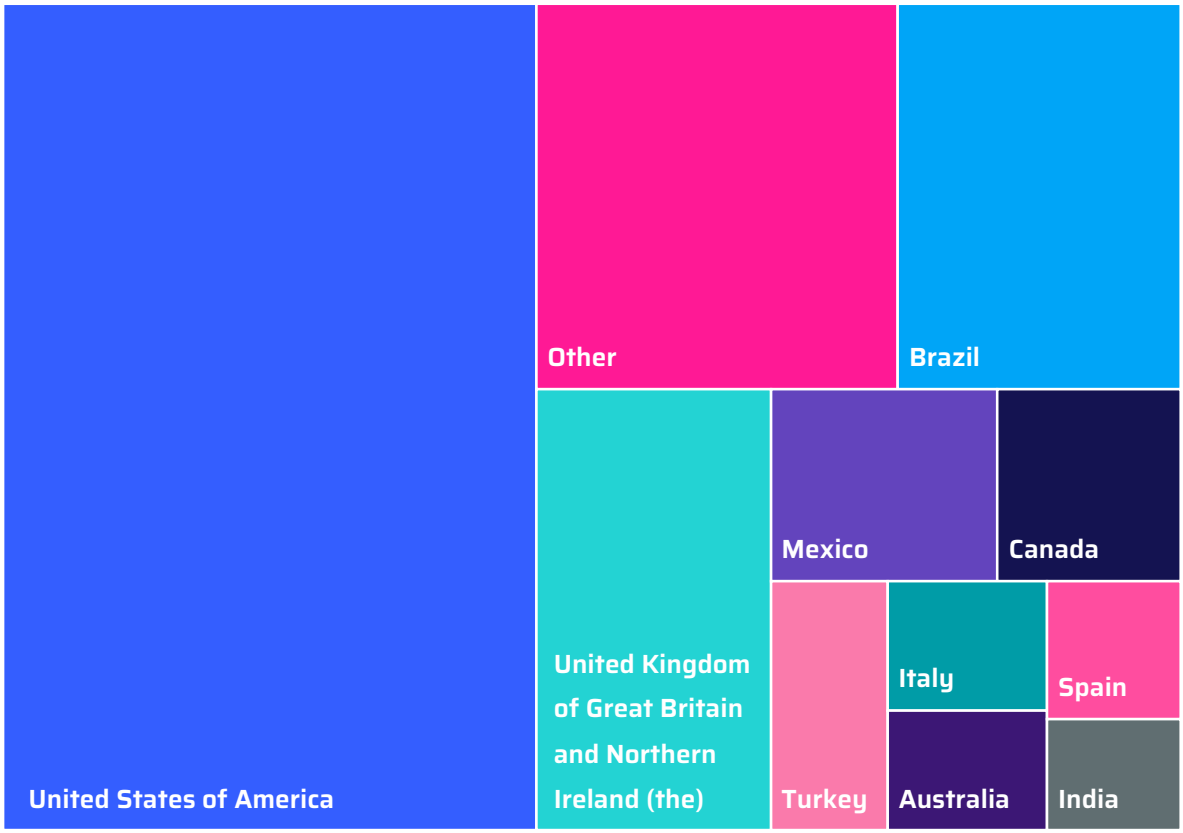


Geographic distribution of compromised cards in H1 2022

Our examination of the global distribution of compromised cards per country of issue revealed that the US is the primary victim of credit card fraud when compared to other countries. Of the total 4,562,998 cards advertised for sale, US-based cards comprised approximately 45.3% (1,855,225) of the total market share. While this marks an 80% decrease in comparison to the similar US portion in H2 2021, this number is decreasing compared to the US segmentation in H1 2021, during which cards issued in the US constituted a 55.9% of the global market share. According to the numbers, the US remains the global leader for compromised payment cards.

Why is this so? There could be several explanations. The United States issues more credit cards per capita than any other country in the world. The latest information shows that there were 249 million US Mastercard credit cards in circulation at the end of March 2021, ~25% of the total world share (725 million).[1] Additionally, the popularity of US-issued cards in the illicit markets of the underground is also driven by a perception that cards issued in the US generally enjoy a higher yield and purchasing power in comparison to cards issued by other countries.

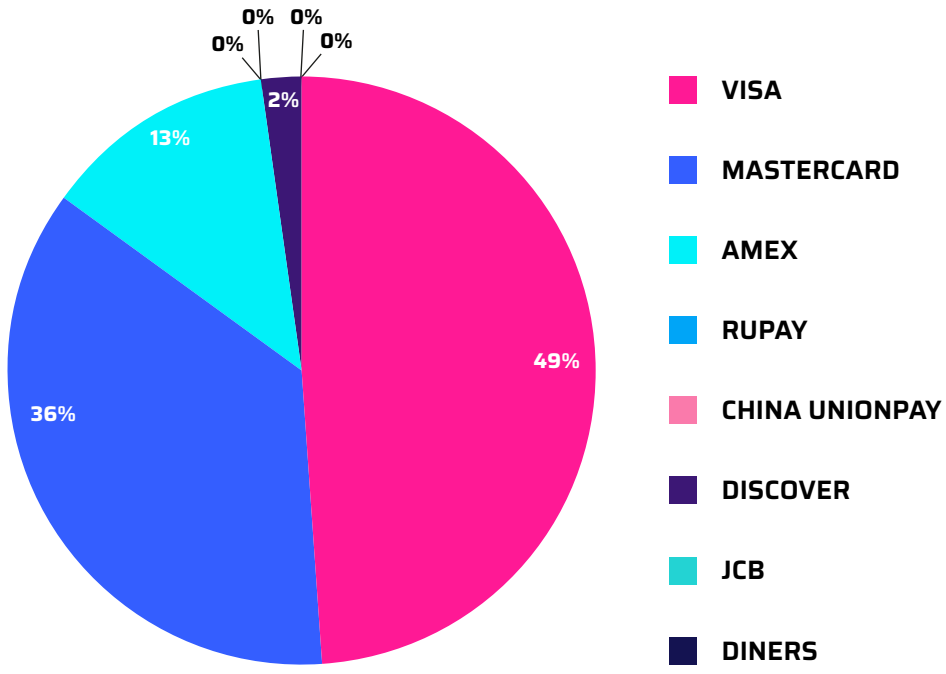
Meanwhile, while Russian actors constitute a large segment of the cybercriminal underground, compromised Russian credit cards are vastly underrepresented on the underground credit card markets, with a mere 5,469 compromised cards detected for sale in H1 2022. This small number is fairly consistent, and is entirely congruent with the unspoken understanding between Russian authorities and the threat actors that operate within their borders: Russian cybercriminals are allowed to operate freely with impunity – as long as they abstain from targeting Russian or CIS citizens.



Geographic distribution of compromised cards in H1 2022

Financial Fraud by Payment Network

Cybersixgill analyzed the distribution of compromised cards issued by the four major payment networks: Visa, Mastercard, American Express, and Discover. Visa, as the largest of the four major networks, also leads the pack in terms of compromised credentials, holding 48.5% of the credit cards offered for sale on the underground.



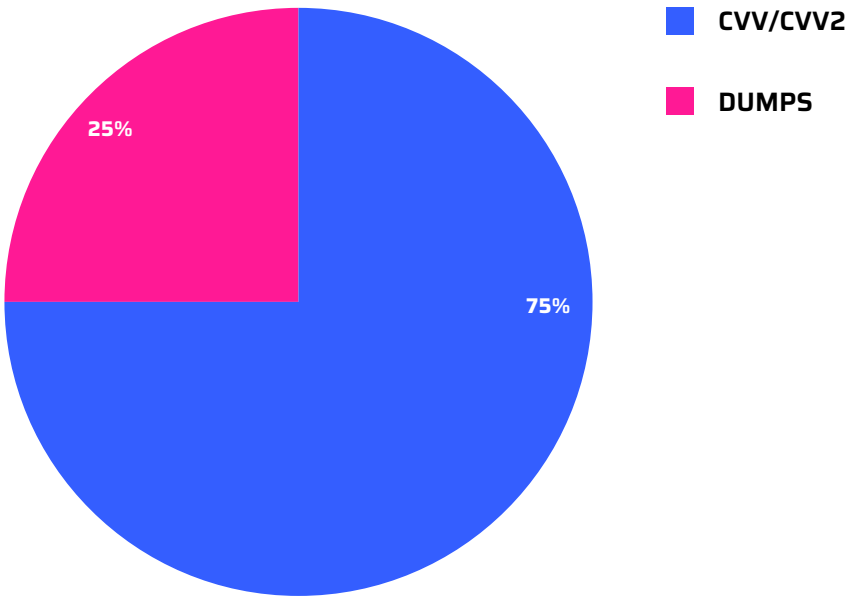
Compromised cards per network

This distribution between the four payment networks falls parallel to their respective order of purchasing volumes, with Mastercard, American Express, and Discover coming in after Visa.[2]

Compromised CVV/CVV2 Cards vs Dumps

On underground credit card markets, there are two predominant forms of compromised cards offered for sale - those categorized as dumps, and those including CVV/CVV2 information. Cards from dumps are used physically (cloned cards, for example) and contain segments of the data related to Track 1 and Track 2, located on the magnetic strip of a card. This data includes the cardholder's name, the account number, card expiration date, BIN, as well as other validating data points used by banks to verify purchases.

CVV/CVV2 information, on the other hand, is not stored in the magnetic strip or on the EMV chip. The CVV/CVV2 is a 3- or 4-digit code on the back of a card, not transmitted when swiped, tapped, or inserted into a POS system. This CVV code is a security feature used to prevent the unauthorized use of a card for "card-not-present" transactions, typically required for online or phone purchases. In H1 2022, cards with CVV/CVV2 data accounted for 75% of compromised cards being advertised, compared to only 25% for dumps. That is a not a minor change from H2 2021, where we saw 84% for CVV vs. 16% for dumps.



Distribution of Dumps vs. CVV/CVV2 in H1 2022

In-person fraudulent activities, whether it be with a skimmer/shimmer or a cloned card, carries a significantly higher risk to the threat actor compared to the anonymity provided by an online purchase. The ability to conduct transactions remotely carries considerably less risk of exposure, making "card-not-present" purchases more attractive and higher in demand. Additionally, cards sold in CVV/CVV2 format may also include additional details, such as home address, email, and other Personally Identifiable Information (PII) that can be exploited by threat actors to use for identity fraud, account takeovers, and other criminal activities. Moreover, CVV/CVV2 cards can be utilized immediately, in contrast to dumps, which require the creation of a fake card.

Conclusion

This report analyzed several trends relating to underground financial fraud in the first six months of 2022, focusing on the 4,562,998 compromised cards offered for sale on illegal credit card markets monitored by Cybersixgill. This represents a steep decrease from the total number of stolen cards identified in H1-2021 (14,185,859) – close to a ~67% decline.

Despite continued efforts by law enforcement agencies, credit card networks, banks, and retailers to improve security, fraudsters are expected to adapt and evolve their skills and techniques, finding new methods to exfiltrate sensitive payment credentials from cards being utilized both virtually and physically. With this in mind, there are certain measures that can be implemented to mitigate the ongoing risks related to financial fraud:

- Monitor bank accounts for suspicious transactions or login attempts. Many banks offer text/email notifications to receive relevant alerts in real-time.
- When receiving order/shipping confirmation emails for purchases made online, (especially during high spending periods, such as the holidays), be careful to navigate to the site directly instead of clicking on links. This will minimize the risk of being redirected to malicious sites.
- Avoid password reuse across multiple accounts and services. Instead, create complex passwords and utilize multi-factor authentication. Use a password manager to keep tabs of your various login credentials and ensure that your passwords are unique for each account.
- Be wary of scams such as fake coupons and promotions. Find those deals on the site rather than clicking on links in emails or ads.
- If you are a retailer, make sure to install chip-enabled point-of-sale systems to protect customers' data. This will decrease the risk of skimmers, as it is more difficult and expensive for fraudsters to try and clone cards that have EMV chips.

Cybersixgill continues to discover and add new markets to its already expansive collection. Having visibility into these sources can help you stay up to date on threats targeting your organization, analyze the trends and perhaps prevent the next attack from happening altogether.

Citations

1. https://www.creditcards.com/credit-card-news/market-share-statistics/

2. https://www.creditcards.com/credit-card-news/market-share-statistics/

Continuously Expose the Earliest Indications of Risk

Cybersixgill continuously collects and exposes the earliest possible indications of risk, moments after they surface on the clear, deep and dark web. Our proprietary algorithms extract data from a wide range of sources, including content from limited-access deep and dark web forums, underground markets, invite-only messaging groups, code repositories, paste sites and clear web platforms, as well as an unparalleled archive of indexed, searchable historical data from as early as the 1990s. This data is processed, correlated and enriched with machine learning techniques to create profiles and patterns of malicious threat actors and their peer networks, delivering critical insight into the nature, source and context of each threat.

Our extensive body of threat intelligence data can be consumed through various solution offerings and integrations, each addressing critical customer pain points and use cases. These solutions are scalable, searchable and seamlessly integrated into existing security stacks, quickly arming enterprises, government and MSSPs alike with accurate, relevant and actionable insights to proactively block threats before they materialize into attacks.

BOOK A DEMO

Follow us

cybersixgill