Underground Financial Fraud H2 2021

Contents

Underground Financial Fraud H2 2021.................................................1
Executive Summary..................................................................................2
Introduction..................................................................................................3
    Geographic Distribution of Compromised Cards....................................4
    Financial Fraud by Payment Network...................................................6
    Compromised CVV/CVV2 Cards vs Dumps..........................................7
Conclusion..................................................................................................8
EXECUTIVE SUMMARY

- During the final six months of 2021 (H2 2021), 14,185,859 compromised payment cards were advertised for sale on underground credit card markets monitored by Cybersixgill. This marks a ~51% decrease from the total number of cards detected for sale on the deep and dark web in H1 2021 (28,939,354).

- 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 56% 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.

- While the United States maintains its unfortunate number one spot within the global market share of compromised credit cards, those originating from Russia keep their place close 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 - so 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, whereby 57.3% of the compromised credentials were issued by Visa, 30.5% by Mastercard, 9.7% by American Express, and 2.4% by Discover.

- Cards sold with CVV/CVV2 information were far more prevalent than those sold as dumps, at a comparative 84% to 16%. 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, whereupon it is purchased by others to be used 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 last six months of 2021 (H2-2021). During this period, 14,185,859\(^1\) compromised cards were offered for sale on underground credit card markets monitored by Cybersixgill. This marks a major reduction in cards offered for sale in our previous H1-2021 (28,934,392) report – a decrease of approximately 51%.

---

\(^1\) Note that these numbers are likely to be revised upwards over the coming months as updates in our collection methodology are introduced.
GEORPHIC DISTRIBUTION OF COMPROMISED CARDS

Our examination of the global distribution of compromised cards per country of issue revealed that the US remains the primary victim of credit card fraud when compared with other countries. Of the total 14,185,859 cards advertised for sale, US-based cards comprised approximately 55.9% (74,297,749) of the total market share. While this marks a 1% increase in comparison to the US portion in the market share in compromised credit cards sold in H1 2021, this number is still a dramatic drop from the US segmentation in H2 2020, during which cards issued in the US constituted a whopping 81.9% of the global market share. Still, despite this decline, at 48%, the US remains the global leader for compromised payment cards, in parallel to previous trends - American card holders remain the primary victims of financial fraud on underground credit card markets.

This trend appears unlikely to change, with the U.S. expected to continue maintaining its unfortunate top spot. This may be attributed to various factors. The United States, in general, issues more credit cards per capita than any other country in the world. While there were 249 million U.S. Mastercard credit cards in circulation at the end of March 2021, the total for the rest of the world was 725 million, reflecting that the U.S. holds a
significant ~25% of the total world share. Additionally, the popularity of U.S.-issued cards in the illicit markets of the underground is also driven by an apparent perception that cards issued in the U.S. 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 974 compromised cards detected for sale in H2 2021. This sparse number is fairly consistent, and is entirely congruent with the unspoken understanding between Russian authorities and the threat actors that operate within their borders, which allows cybercriminals to operate freely with impunity – as long as they abstain from targeting Russian or CIS citizens.

Figure 2: Geographic distribution of compromised cards in H2 2021

---

2 https://www.creditcards.com/credit-card-news/market-share-statistics/
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 57.6% of the credit cards offered for sale on the underground.

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.\(^3\) It is particularly interesting to note that American Express cards for sale on the underground plummeted from the abnormally high 38% of the market share observed in H2 2020 to 11.7% in H1 2021 and to 9.7% in H2 2021. This anomaly in H2 2020 may be explained by the fact that AMEX holders typically come from higher income households, where credit card usage may have been less impacted during the financial consequences of the pandemic.

\(^3\) [https://www.creditcards.com/credit-card-news/market-share-statistics/](https://www.creditcards.com/credit-card-news/market-share-statistics/)
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 H2 2021, cards with CVV/CVV2 data accounted for 83.6% of compromised cards being advertised, compared to only 16.4% for dumps. That is a drastic change from H1, were we saw 58% for CVV vs. 42% for dumps.

In-person fraudulent activities, whether it be with a skimmer/shimmer or a cloned card, carries a significantly higher risk to the threat actor when 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 last six months of 2021, focusing on the 14,185,859 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 H2-2021 (28,934,392) - close to a ~51% 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.