sixgill

AUGUST 20, 2020

SIXGILL REPORT

# Underground Financial Fraud H1 2020

# Underground Financial Fraud H1 - 2020

## EXECUTIVE SUMMARY

- During the last six months of 2020 (H1 – 2020), **45,130,117** compromised payment cards were offered for sale by threat actors on illegal credit card markets monitored by Sixgill in the deep and dark web. This is a decrease of 40% comparing to H2 – 2019, where 76,230,127 cards were offered for sale.
- In our understanding, the main reason for this drastic decrease is law enforcement agencies' operations. In March 2020, Russian law enforcement took down many prominent dark web credit card markets, which led to a significant reduction in the amount of cards available in the first half of 2020.
- As the Covid-19 pandemic continues and e-commerce sales soar in the US, compromised cards originating from the United States constituted 49% of the global market share of compromised payment cards.
- Analyzing the four major payment networks, Visa had the most compromised cards available on the dark web at 55%. Mastercard came in second at 33%, followed by American Express (6%) and Discover (1%). There was no movement in payment network rankings when compared to H2 – 2019.
- Covid-19 lock downs and quarantines have prevented threat actors from gaining frequent access to point-of-sale systems located at stores and gas stations. This appears to have directly impacted the distribution of card dumps as threat actors have halted card cloning services and shimmer/skimmer sales. Card dumps accounted for just 38% of payment cards for sale in H1 – 2020.

## INTRODUCTION

2020 has been an extraordinary year. The new reality of Covid-19 quarantines and shutdowns diverted our attention and put what seems like "real life" largely on hold. During this time, the digital underground continued business as usual, and we witnessed as threat actors continued, without interruption, their trade of malicious content, leaked data, and payment cards.

This report will examine financial fraud activity that took place in the deep and dark web during the last six months of 2020 (H1 – 2020). During this period, **45,130,117** compromised cards were offered for sale in credit card markets monitored by Sixgill in the underground.

In our H2 – 2019 report, we examined 76,230,127 compromised cards being offered for sale during the period of July 1 2019 – Jan 1, 2020. Sixgill observed a 40.7% decrease in compromised cards when comparing the two periods. This significant decrease could be the result of a combination of factors. The decrease could be due to fewer cards being obtained through physical devices like shimmers or skimmers, devices deployed on point-of-sale systems found in stores and gas stations, and more people staying home due to the pandemic. It could also be the result of law enforcement taking down several credit card markets over the last several months. This report will investigate both the potential causes and bring to light any evidence related to the reduction in payment cards available on the deep and dark web.

## ANALYSIS BY CREDIT CARD MARKET

As seen in figure 1, the H2 – 2019 underground financial report identified three top markets that held nearly 30% of all compromised payment cards collected by Sixgill.

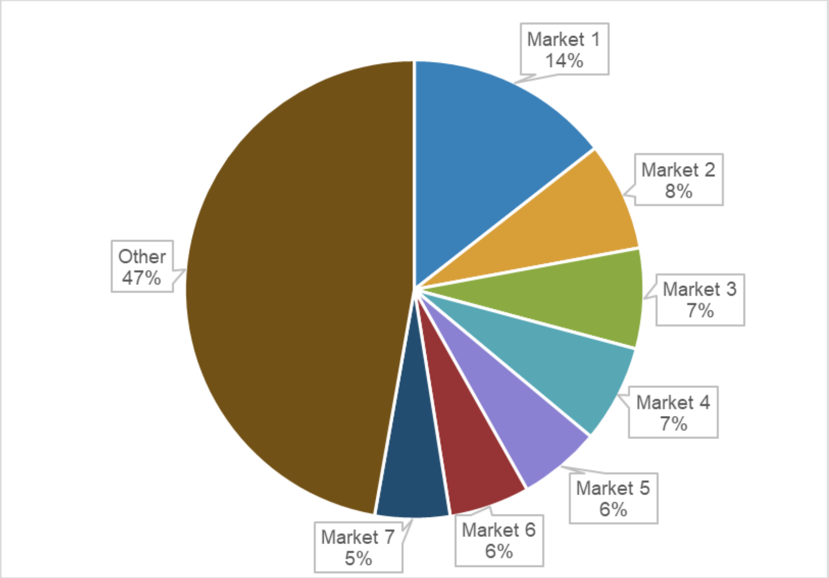


**Figure 1: Segmentation of compromised cards sold in the underground by market during H2 – 2019.**

H1 – 2020 saw many of the same markets selling the 45,130,117 available cards; however, it was immediately apparent that there are new leaders in the most cards for sale (Figure 2).

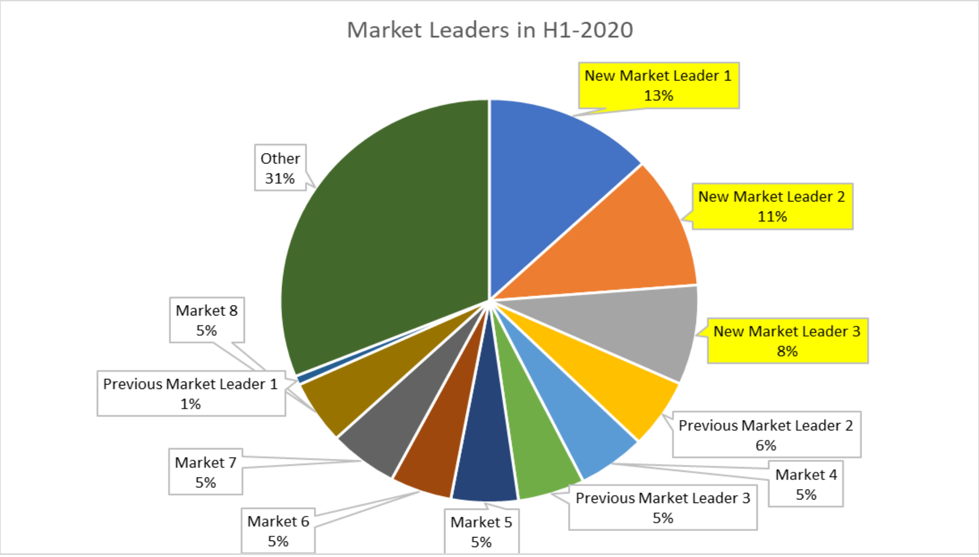


**Figure 2: Segmentation of compromised cards sold in the underground by market during H2 – 2020.**

*Previous Market Leader 1* plummeted from the top spot at 14% of the market in H2 – 2019 to just 1% of the market in H1 – 2020. Meanwhile, the new H1 – 2020 market leaders all made significant gains.

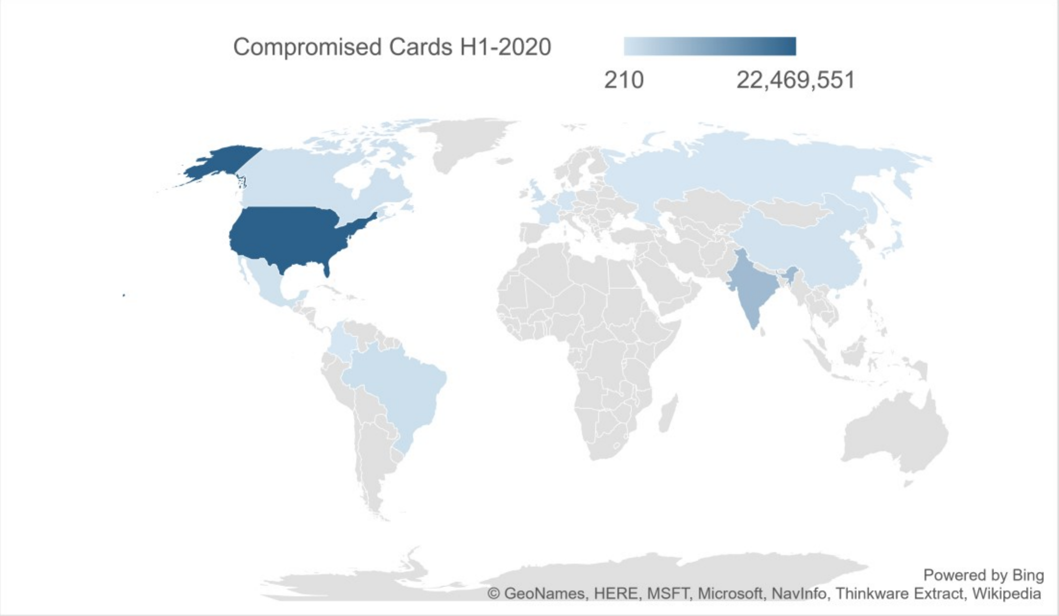
| Market | H2 - 2019 | H1 - 2020 |
|---|---|---|
| New Market Leader 1 | 7% | 13% |
| New Market Leader 2 | <1% | 11% |
| New Market Leader 3 | <1% | 8% |
| Previous Market Leader 1 | 14% | 1% |
| Previous Market Leader 3 | 7% | 5% |

| | | |
|---|---|---|
| Market | 6% | 5% |
| Previous Market Leader 2 | 8% | 6% |
| Market | 6% | 5% |

Fortunately, there is a positive explanation for these drops. In March 2020, Russian federal investigators charged at least 25 people for operating international credit card rings and shut down dozens of dark web marketplaces.[1]

The numerous market shutdowns significantly contributed to the H2 – 2019 report which helps explain why H1 – 2020 saw a 40.7% decrease in compromised cards. In H2 – 2019, these markets accounted for 54%, or, 41,504,730 of all compromised cards collected by Sixgill. For just the nearly three months they were still active in H1 - 2020, these markets accounted for 45%, or, 20,376,137 of the compromised cards collected, which suggests that they were operating at or around the same pace as in H2 – 2019 had they been active the entire half.

## GEOGRAPHIC DISTRIBUTION OF COMPROMISED CARDS



Powered by Bing
© GeoNames, HERE, MSFT, Microsoft, NavInfo, Thinkware Extract, Wikipedia

[1] https://krebsonsecurity.com/2020/03/russians-shut-down-huge-card-fraud-ring/

**Figure 3: Geographic distribution of compromised cards in H1 – 2020.**

As was observed in H2 – 2019, cards originating from the United States remained available on the dark web at a much higher rate than other countries. From the 45,130,117 cards that were available, 49%, or 22,469,551 cards originated from the United States. American credit card holders still hold a large share of the total cards in circulation around the world; thus, it is of no surprise that America continues to lead the way in compromised cards on the dark web. Additionally, stay-at-home orders due to Covid-19 have not seemed to have had an adverse impact on online sales for American consumers—in other words, Americans are not using their credit cards any less than usual. In fact, compromised CVV cards made up 62% of all compromised payment cards on the dark web. Grocery delivery services such as Instacart, have greatly benefited from the virus, growing by nearly 500% since March 2020. More Americans are ordering their groceries to avoid contact with others and are spending more on online groceries each successive week of the crisis.[2] Still, due to closure of the previously mentioned markets, the actual number of compromised cards decreased for every country. In H2 – 2019 the US saw 49,190,022 cards in the underground, as opposed to 22,469,551 in H1 – 2020, a 54% decrease.

Increased e-commerce sales during the pandemic leaves plenty of opportunity for fraudsters to take advantage through e-skimming attacks by infecting checkout pages to collect customer information. This is similar to the increased sales around holiday seasons which attracts fraudsters to e-commerce sites. A notable attack last year was on the firearms maker's website, *America Outdoor Brands*, where fraudsters infected the checkout page with an e-skimming trojan like MageCart.[3] The attack only affected about 780 people, but still a successful attack and one that should be used as a warning for other e-commerce sites.

Some are suspicious of hackers that have established "beachheads" or gained entry to multiple smaller retailers. These small to medium-sized retailers may have experienced less sales during the pandemic causing the hackers to hold off on deploying their e-skimmers until they see an increase in sales.[4] If they do, we may witness an increase in compromised payment cards for sale in the underground.

Despite the 40% drop in total cards available, there was slight movement in the country standings when compared to H2-2019 (Figure 4). India remained in second for most compromised cards at 15.93% while

[2] https://www.nytimes.com/interactive/2020/05/13/technology/online-shopping-buying-salescoronavirus.html
[3] https://www.cnbc.com/2020/01/31/e-skimming-cyberattack-is-growing-along-with-onlineshopping.html
[4] https://krebsonsecurity.com/2020/06/covid-19-breach-bubble-waiting-to-pop/

Brazil (2.78%) overtook China (1.21%) for the third spot. Portugal was added to the list of countries observed; however, accounted for a very small percentage of compromised cards at 0.049%.

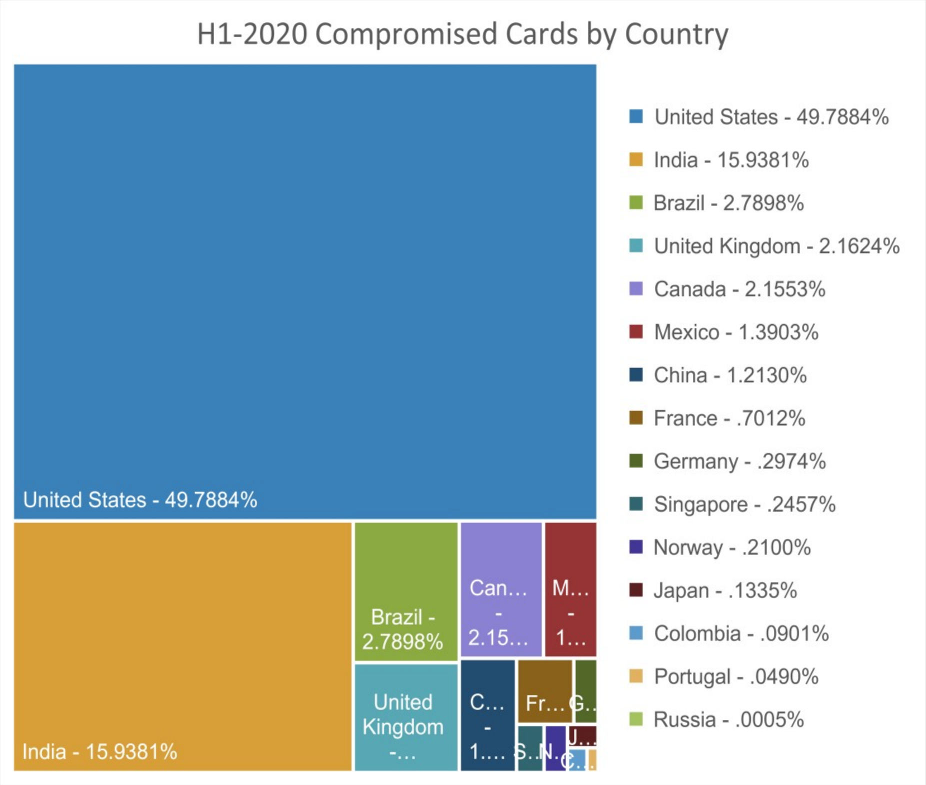


**Figure 4: Geographic distribution of compromised cards in H1 – 2020.**

Russian cards remained at the bottom of the list with .0005%, or 210 total cards available. This continues to reinforce the idea that Russian threat actors are allowed to operate with immunity as long as the government holds the same interests and they do not attack Russian citizens. However, this leaves questions as to why the Russian markets were taken down by Russian law enforcement. It appears that President Putin recently provided his intent to crack down on Russian cybercrime, which may be specifically referring to those that commit crimes against Russians.[5] When the raids on the persons running the markets occurred, Russian law enforcement seized firearms, drugs, and fake identities that included Russian Federation passports and law enforcement officer IDs, indicating that fraudsters overstepped the bounds of impunity, a strong reminder for Russian threat actors to not target Russia.

[5] https://securityboulevard.com/2020/03/following-putin-order-fsb-cracks-down-on-russiancredit-card-marketplaces/

## FINANCIAL FRAUD BY PAYMENT NETWORKS

Sixgill analyzed the distribution of compromised cards according to the four major payment networks of 2019; Visa, Mastercard, American Express, and Discover.[6] Additionally, the major credit card networks for both China and India (UnionPay and RuPay, respectively) were included (Figure 5). There was no movement in rankings for the four major networks since our last report on financial fraud in the underground. Visa remains ahead of all the competition in the card network industry.[7] Mastercard is slightly behind in market share; however, both remain the bulk of payment cards available on the underground. Additionally, although India was second among compromised cards by country, RuPay cards made up just 1% of the distribution by networks. That said, India also participates in the four major networks, particularly Visa and Mastercard.[8]

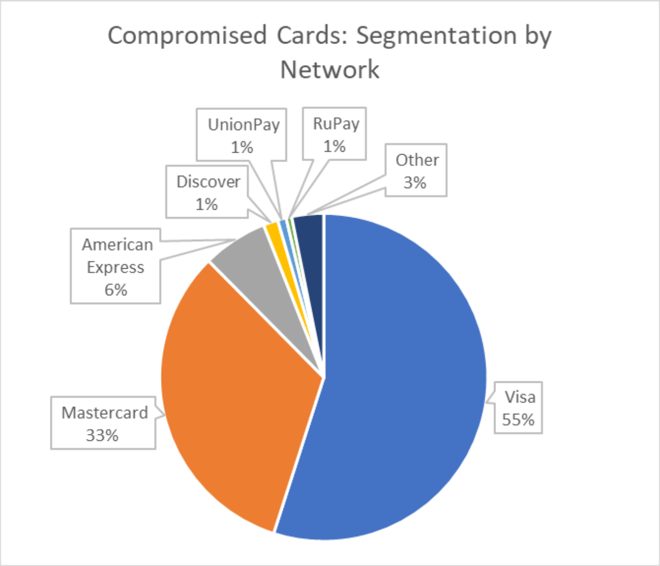


**Figure 5: Distribution of compromised cards by payment network in H1-2020.**

## COMPROMISED CVV/CVV2 CARDS VS DUMPS

Dark web credit card markets have two primary types of compromised payment cards offered for sale, dumps and CVV/CVV2. Cards obtained from dumps are used physically (in person) and contain segments of the data related to Track 1 and Track 2, located on the magnetic strip. In H1 – 2020, dumps accounted for 38% of compromised cards available for sale in the underground (Figure 6). Furthermore, cards with

[6] https://www.businessinsider.com/credit-card-networks-payment-list

[7] https://www.businessinsider.com/credit-card-networks-payment-list

[8] https://www.paisabazaar.com/credit-card/credit-card-networks-visa-mastercard-amex-discover-rupay/#:~:text=The%20major%20credit%20card%20networks,the%20cards%20and%20payment%20system.

CVV 62%

compromised CVV/CVV2 information were much more accessible, accounting for 62% of the compromised cards for sale in the underground.

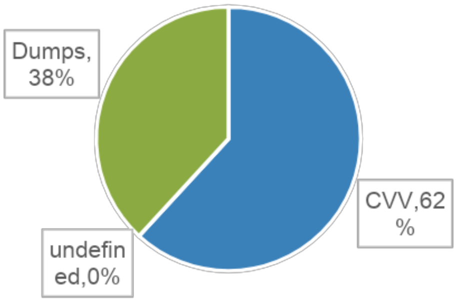
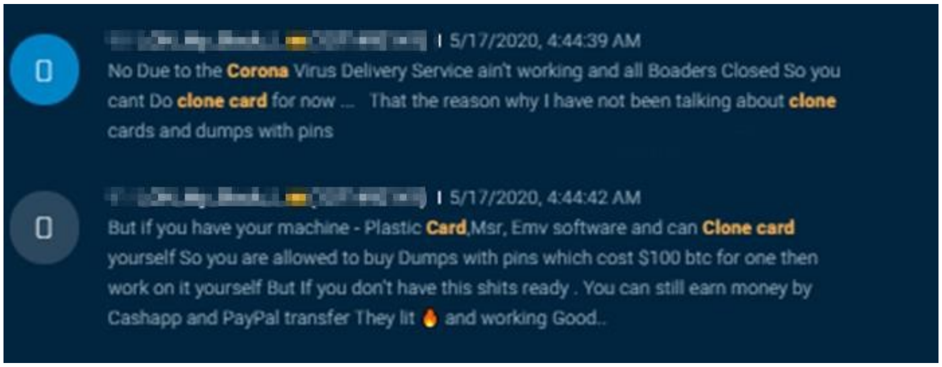


**Figure 6: Distribution of dumps vs CVV in H1-2020**

## COVID-19 IMPACT ON DUMPS

With the ongoing pandemic, physical dumps and card cloning may not be as high in demand, nor are they acquiring as many cards as observed previously. Due to lockdowns and closures, threat actors have less access to brick and mortar stores, ATMs, and other places with point-of-sale systems where they can use cloned cards. Sixgill has observed threat actors in the underground posting announcements about their dumps (Figure 7).

The threat actor announced that their card cloning service will be temporarily disabled due to the impact of Covid-19. However, they do still encourage clients to purchase dumps if they have their own means of cloning cards.

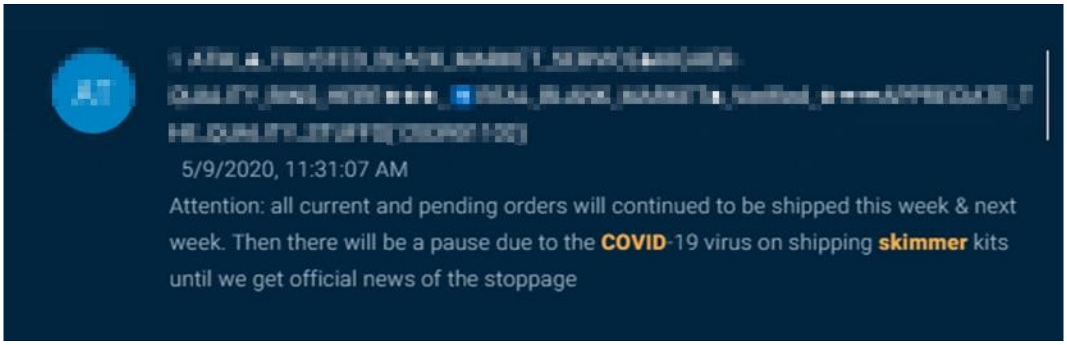


[redacted] | 5/17/2020, 4:44:39 AM
No Due to the **Corona** Virus Delivery Service ain't working and all Boaders Closed So you cant Do **clone card** for now ... That the reason why I have not been talking about **clone** cards and dumps with pins

[redacted] | 5/17/2020, 4:44:42 AM
But if you have your machine - Plastic **Card**,Msr, Emv software and can **Clone card** yourself So you are allowed to buy Dumps with pins which cost $100 btc for one then work on it yourself But If you don't have this shits ready . You can still earn money by Cashapp and PayPal transfer They lit 🔥 and working Good..

**Figure 7: A threat actor posting announcements about credit card dumps.**

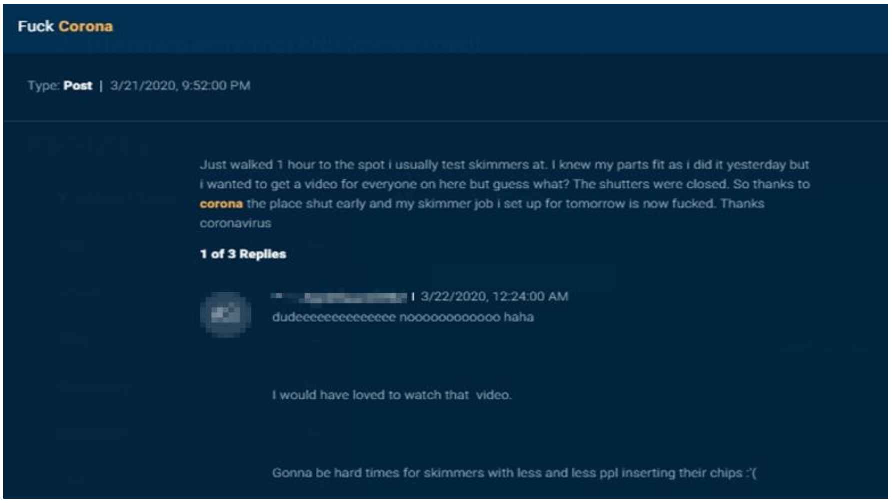
Card cloning is not the only service to pause during the pandemic. In fact, the very means of acquiring track 1 and 2 information through skimming and shimming kits, devices installed on point-of-sale systems to capture card information when inserted or swiped, has been impacted by the virus. The following threat actor announced in May 2020 that they would be pausing all future orders and shipments of skimmer kits due to the virus (Figure 8).



[redacted]
5/9/2020, 11:31:07 AM
Attention: all current and pending orders will continued to be shipped this week & next week. Then there will be a pause due to the **COVID**-19 virus on shipping **skimmer** kits until we get official news of the stoppage

**Figure 8: A threat actor posting an announcement regarding pauses in services.**

Others in the underground found out that they would not be able to continue their skimming the hard way, as did the following threat actor when they walked an hour to their usual skimming location only to find that it had been closed due to the pandemic (Figure 9).



Fuck Corona

Type: **Post** | 3/21/2020, 9:52:00 PM

Just walked 1 hour to the spot i usually test skimmers at. I knew my parts fit as i did it yesterday but i wanted to get a video for everyone on here but guess what? The shutters were closed. So thanks to **corona** the place shut early and my skimmer job i set up for tomorrow is now fucked. Thanks coronavirus

**1 of 3 Replies**

[redacted] | 3/22/2020, 12:24:00 AM
dudeeeeeeeeeeeeeee nooooooooooooo haha

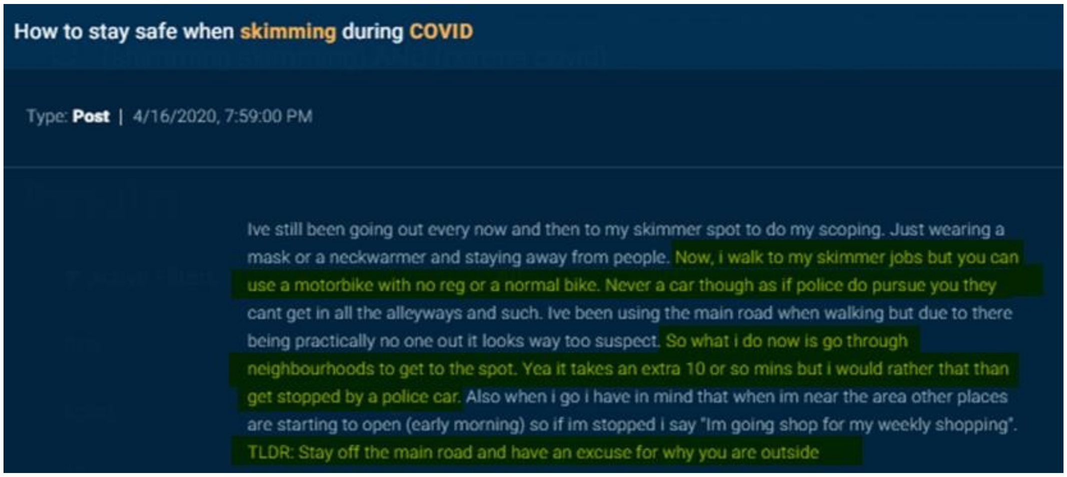
I would have loved to watch that  video.

Gonna be hard times for skimmers with less and less ppl inserting their chips :'(

**Figure 9: Threat actor posting about their difficulties with carding during the pandemic.**

One of the threat actors that replied also acknowledged the impact of the virus on skimming as less people will be using point-of-sale systems at physical locations (Figure 9).

Still, the poster is determined to continue their fraudulent activities as seen in a more recent post on a dark web forum (Figure 10).



How to stay safe when skimming during COVID

Type: **Post** | 4/16/2020, 7:59:00 PM

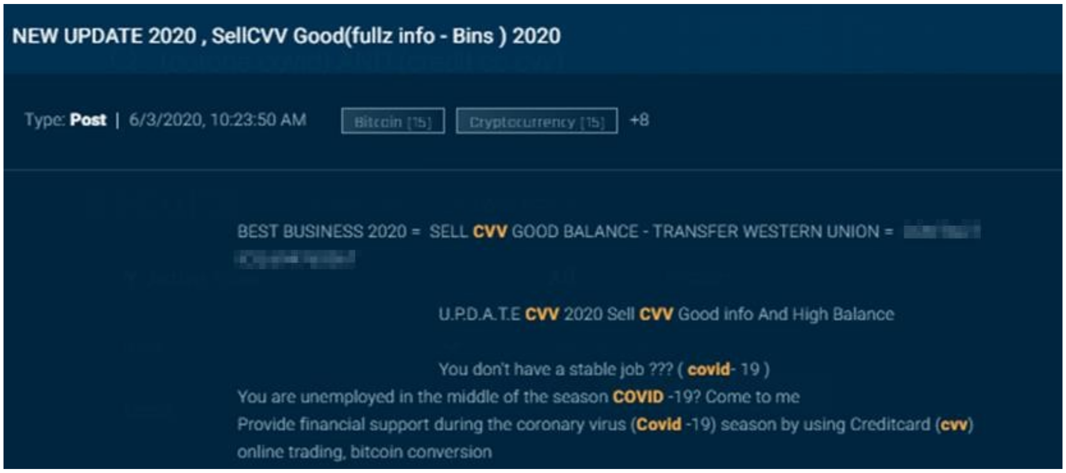
Ive still been going out every now and then to my skimmer spot to do my scoping. Just wearing a mask or a neckwarmer and staying away from people. Now, i walk to my skimmer jobs but you can use a motorbike with no reg or a normal bike. Never a car though as if police do pursue you they cant get in all the alleyways and such. Ive been using the main road when walking but due to there being practically no one out it looks way too suspect. So what i do now is go through neighbourhoods to get to the spot. Yea it takes an extra 10 or so mins but i would rather that than get stopped by a police car. Also when i go i have in mind that when im near the area other places are starting to open (early morning) so if im stopped i say "Im going shop for my weekly shopping". TLDR: Stay off the main road and have an excuse for why you are outside

**Figure 10: Threat actor advising others on how to be safe during the pandemic while carding.**

In this post, the threat actor provides others with their own guidelines on how to properly protect themselves from the virus as they visit each of their skimming locations, such as by wearing a mask or neck warmer while keeping distance from others while they are planting or retrieving their devices.

## COVID-19 IMPACT ON CVV/CVV2

The virus appears to have less of an adverse impact on threat actors engaging in CVV/CVV2 sales. In a post by the following threat actor, they are promoting their business by using the pandemic as a method to generate sales and potentially to attract some new employees to engage in online trading and bitcoin conversion (Figure 11).



NEW UPDATE 2020 , SellCVV Good(fullz info - Bins ) 2020

Type: **Post** | 6/3/2020, 10:23:50 AM

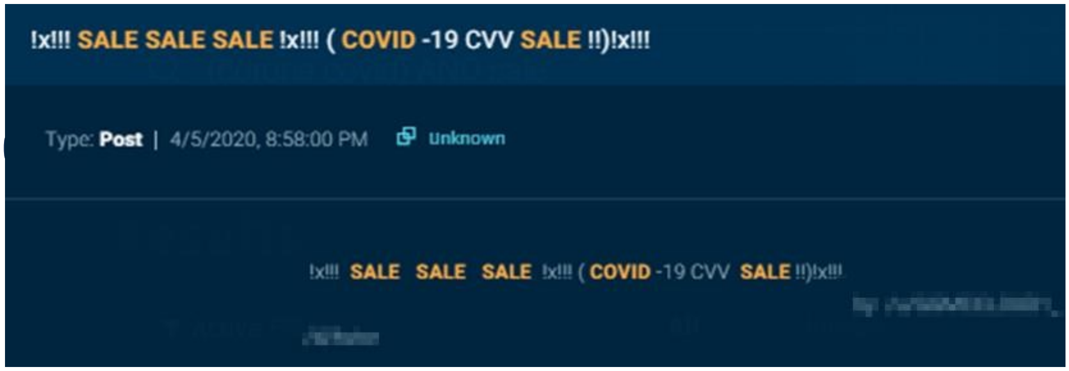
BEST BUSINESS 2020 = SELL **CVV** GOOD BALANCE - TRANSFER WESTERN UNION = [redacted]

U.P.D.A.T.E **CVV** 2020 Sell **CVV** Good info And High Balance

You don't have a stable job ??? ( **covid**- 19 )
You are unemployed in the middle of the season **COVID** -19? Come to me
Provide financial support during the coronary virus (**Covid** -19) season by using Creditcard (**cvv**)
online trading, bitcoin conversion

**Figure 11: Threat actor promoting their carding business during the pandemic.**

Additionally, others were observed offering discounts due to the pandemic as seen in this post on a dark web where a threat actor was promoting their vendor pages on a separate dark web market (Figure 12).



!x!!! **SALE SALE SALE** !x!!! ( **COVID** -19 CVV **SALE** !!)!x!!!

Type: **Post** | 4/5/2020, 8:58:00 PM

!x!!! **SALE SALE SALE** !x!!! ( **COVID** -19 CVV **SALE** !!)!x!!!

[redacted]

[redacted]

Figure 11: Threat actor offering discounts during the pandemic.

# CONCLUSION

This report analyzed different trends related to underground financial fraud in H1 – 2020, focusing on the **45,130,117** compromised cards that were offered for sale in illegal credit card markets monitored by Sixgill. Compared to the 76,230,127 cards observed in H2 – 2019, the 40.7% decrease is the result of many credit card market takedowns by Russian law enforcement, and potential impacts on the collection of dumps from the Covid-19 outbreak. Although many markets were terminated, Sixgill continues to add new markets that pop-up in the underground as they attempt to take advantage of the sudden reduction of competition, as well as continues to monitor already existing markets that may become more prominent.

As the pandemic continues to force sales to online transactions, threat actors will likely focus their efforts on CVV/CVV2 data and infecting merchants with eskimming malware such as Magecart. Here are several recommendations to help protective one's self from cyber fraud:

- Monitor bank accounts for suspicious transactions or login attempts. Many banks allow for text/email notifications so stay alert in real-time.
- If you make a purchase online and receive an order/shipping confirmation email, navigate to the site directly instead of clicking on links. This will minimize the chance of being redirected to malicious sites.
- Do not reuse passwords. Use a password manager 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 yours and your customers' data. This will greatly decrease the risk of skimmers because it is more difficult and expensive for fraudsters to try and clone cards that have EMV chips.