

 FLASHPOINT

Joker's Stash Post-Mortem

Where Will the Cybercriminals Go?

FEBRUARY 15, 2020

On Friday, January 15, 2021, the operators of Joker's Stash, among the world's largest illicit card shops, made the unexpected announcement that the shop **would shut down** in another 30 days.

The decision marks the closure of one of the largest—by both card volume and quality—and longest-standing card shops in history, reigning at a time of rapid growth for the card fraud market overall along with steep rises in related illicit transactions.

This research paper summarizes the rise and fall of Joker's Stash, and consolidates the viewpoints of Flashpoint analysts and other subject matter experts regarding how the card fraud industry will evolve following the shop's closure.

The Rise and Fall of Joker's Stash

Joker's Stash was not the first illicit card shop and it certainly won't be the last. The first material surge in online card fraud activity occurred in the mid-1990s, coinciding with the initial wave of Web 1.0 as the first eCommerce sites began accepting electronic credit card transactions to run on their servers.

As the Internet matured, so too did cybercrime. Once starting with bulletin board services (BBS) and internet relay chat (IRC), fraudsters transitioned to encrypted cybercrime forums, dark web marketplaces, and specialized shops to conduct their illicit business. Carding even spawned entire new cybercriminal markets such as personal information lookups, brute-forced accounts, SOCKS proxies, and anti-detect browsers, just to name a few.

Joker's Stash Demise: A Timeline

Over the past year, and particularly during the second half of 2020, both the volume and quality of Joker's Stash inventory began to dwindle (see Figure 1). The shop experienced disruptions and downtime, and dealt with an increasingly volatile market due to the global coronavirus pandemic and other market shifts.

In order to fully understand how and why the operators made their decision to shut down their popular shop, it's important we review how Joker's Stash came to be and the major events that ultimately affected its business trajectory:



2011 to 2014: As small illicit carding communities went mainstream and grew to critical mass over the preceding decade, law enforcement took notice and began taking aggressive action to dismantle these then-booming illicit marketplaces—including Carders' Forum, Carders Market, CarderPlanet, DirectConnection, Liberty Reserve, and Silk Road. As a result, the list of **the 'dons' and the 'capos' of the carding mafia** dwindled, creating a noticeable void in online carding shops and paving the way for Joker's Stash to emerge with few competitive threats.



October 7, 2014: In the wake of major credit card breaches that, in sum, exposed 10s of millions of cards, Joker's Stash opened for business. Around the same time, JokerStash—the user handle representing the owner of the similarly-named shop—first appeared on underground forums and began promoting the new marketplace. From its inception, Joker's Stash offered large volumes of uniquely and highly valid cards not available anywhere else online.



2014 to 2017: Joker's Stash offered cleverly-worded credit card breaches that became events for the entire carding community, labeling its card inventory as "zero day dbs," and "exclusive self-hacked bases."



September 2017: Joker's Stash begins to exclusively host its shops and associated infrastructure via blockchain DNS. Up to this point, the shop relied on private deep web domains and dark web Tor links, but these methods were insufficient for a variety of reasons, including operational availability issues, external abusers, and exposure to law enforcement. JokerStash claimed that blockchain DNS, "is perfect bcoz its impossible to abuse and it's fully resistant to domain locks."






2019 to 2020: From February 2019 to February 2020, five major data breaches provided high volumes of card inventory on Joker's Stash that carried the marketplace into July 2020.



July 2020 to December 2020: Shop activity fell steeply over the second half of 2020. Even the addition of new inventory from the "BlazingSun" breach didn't curtail the downshift in shop activity.



December 16, 2020: Flashpoint analysts first noticed issues accessing Joker's Stash on December 8th. Later the following week, on December 16th, Joker's Stash main domain displayed a takedown notice from the FBI and Interpol. Joker's Stash acknowledged that law enforcement took over an external proxy server, but reassured its user base that no shop data was seized.

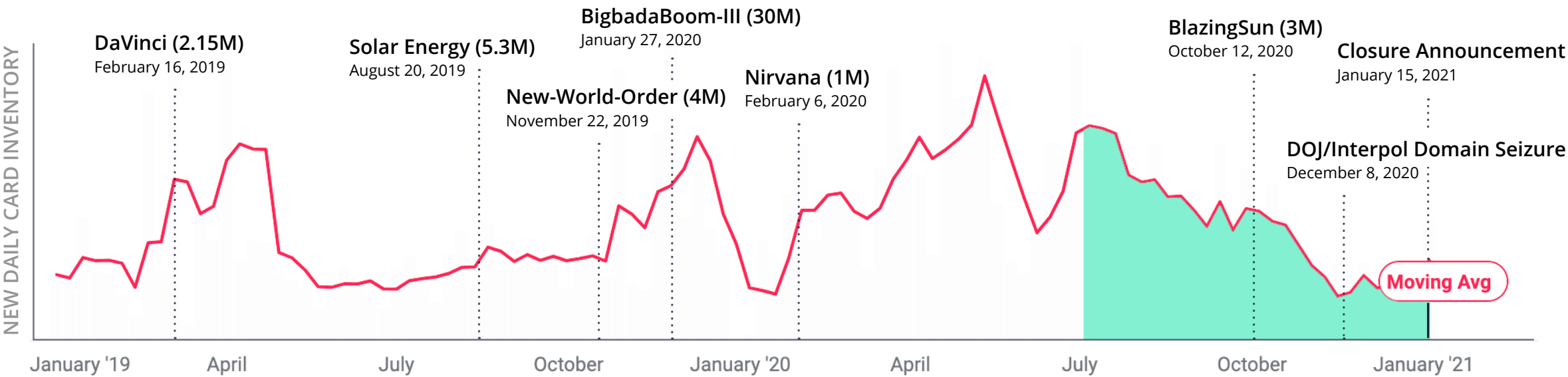
-  **January 15, 2021:** Shop operators announced that **Joker's Stash would shut down** over the next 30 days.
-  **February 3, 2021:** Flashpoint analysts discovered that operators had recently deleted chat channels and threads previously used to facilitate community communications and announcements.
-  **February 15, 2021:** While the shutdown may have occurred for good on February 3rd, February 15th is the date that Joker's Stash initially indicated that it would permanently take all remaining operations offline.

Operators Likely Planned Shutdown Months in Advance

Based on the data, it's clear that Joker's Stash activity began to fall precipitously starting in July 2020. JokerStash, the shop administrator, built a reputation based on the shop's reliable and quick customer responses. Since at least the end of July 2020, however, JokerStash's normally speedy fielding of comments, complaints, and feedback across top tier forums began to ebb and grew increasingly worse and more sporadic in the following months.

JokerStash's once infamous and routine "breaches" announcements of new stolen credit card data stolen from physical point-of-sale terminals became sparse, with only one major announcement in the second half of 2021. And even this singular breach, BlazingSun, and its three million cards paled in comparison; it amounted to less than one-tenth of the cards contained in its past breaches, like Big-Badaboom-III.

For a detailed chart of all of Joker's Stash's biggest stolen card breaches, please click [here](#)



Joker's Stash Notoriety Tied to Its Customer Service

In a community built on trust, it's striking that the shop's founder, JokerStash, was largely unknown from the outset. The person(s) behind JokerStash had no other known aliases or community presence tied to their online identity prior to establishing Joker's Stash. They claimed to be of distinguished provenance, stating, "yes, a lot of years before i opened my Stash i stayed behind the scene and most of you guys keep using my stuff for tens of years, believe me."

Instead, JokerStash let the quality and reliability of the Joker's Stash shop speak for itself. JokerStash built the shop's reputation fast, quickly becoming known for the high-quality of the shop's card data, favorable seller policies, and responsiveness to inform customers' opinions.

Six Years of Reliable Operations, A Lifetime in Carding Circles

In a cybercrime landscape filled with uncertainty, Joker's Stash provided a refuge of relative stability. While other illicit marketplaces—like AlphaBay, Empire, Dream, Hansa, and Wall Street—rose and fell due to exit scams, law enforcement shutdowns, and unreliable infrastructure, Joker's Stash consistently remained in operations with few blips in service even worth noting.

Joker's Stash also exhibited innovation through its pioneering of Blockchain DNS for its infrastructure hosting needs. Since 2017, Joker's Stash has required users to install browser plugins to access the shop. JokerStash favored Blockchain DNS, "Because it's decentralized and has no central authority, it's resistant to domain locks and other abuse." Blockchain-DNS allows the user, instead of asking their ISP for the location of a specific domain, to go through nodes in a blockchain network.

Many Factors Influenced the Call to Shut Down

With little detail about JokerStash's decision to shut down, and why now, we are left to speculate the reasons for ourselves. It goes without saying, few fraud venues ever make a graceful exit; it's part of being in the cybercrime business. And after six years in continuous operation, increased law enforcement scrutiny, consumer activity increasingly moving online, and a global pandemic to expedite all of these trends: the writing was clearly on the wall.

Closure Inevitable as eCommerce Picks Up Amid Pandemic

Unlike other shops that were forced into closure or ran exit scams to profit on the way out, JokerStash claims it is shutting down on their own

terms—allegedly making a concerted decision to shutter its doors based on market trends, a global pandemic, and mounting financial risk. In particular, several factors likely influenced Joker's Stash's closure:

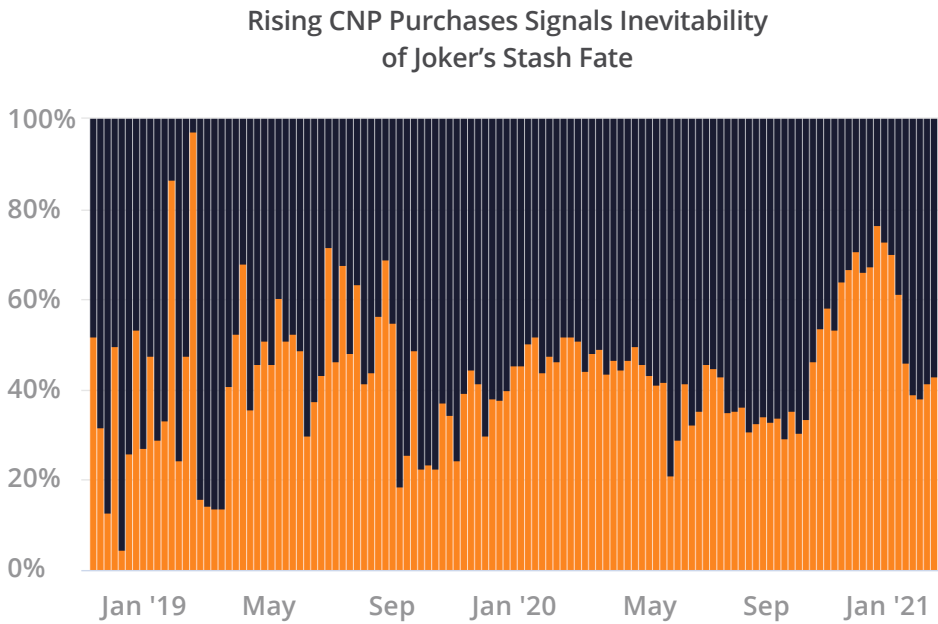
- 1 Changing consumer buying habits devalue Card Present (CP) data.** As consumer spending increasingly shifts to online shopping and entertainment services, the opportunities to run CP scams are falling. As a result, the value of stolen CP data—a staple product on Joker's Stash—continues to fall as fraudsters look to other fraud methods.
- 2 Joker's Stash can't monetize Card Not Present (CNP) at the same scale as CP.** While reason would follow that Joker's Stash could offset any lost value in CP data with increased CNP sales, that isn't what took place. While, yes, CNP purchases on Joker's Stash have been on the rise in comparison to CP purchases, this is far more likely a result of falling shop activity overall and falling CP purchases in particular (see Figure 2). In large part, this is because CNP supply is more limited and related fraud tactics more difficult to execute at scale.

3 Coronavirus accelerated eCommerce and consumer trends. With the now almost year-long global coronavirus pandemic still ongoing, we've seen material shifts in consumer spending transition online. In particular, this has dramatically reduced in-person physical transactions typically conducted at, or in close proximity to, restaurants, gyms, hotels, airlines, and entertainment venues (and many others). While online payments had already been moving in this direction, the global pandemic accelerated it, and in doing so, further devalued associated card fraud techniques.

4 New security protections and better fraud prevention techniques. Increased protections on security cards are also increasing friction for carders. For instance, the required use of chip-and-pin on payment terminals forces renders fraud techniques that leverage CP data useless. Additionally, new payment methods like contactless payments require threat actors to be agile and introduce further complexity into pilfering and cashout scams. Meanwhile, fraud teams at financial institutions continue to improve their fraud detection and prevention techniques, further minimizing the frequency or size of potential fraud payouts.

5 Increasing international law enforcement scrutiny. In November 2020, Joker's Stash experienced a temporary shutdown, which they claimed was due to a "heavy COVID infection" but is widely believed to be related to a coordinated law enforcement

takedown operation. Prior to that, on March 24, 2020, the Federal Security Service (FSB) of the Russian Federation announced that it had detained more than thirty members of a large-scale illicit carding syndicate led by threat actor "Flint24" (aka, "Alexey Stroganov"). Following this enforcement raid, community chatter signals that Joker's Stash operators were among the 30 detainees, despite their explicit denial of the speculation.



Closing Thoughts

JokerStash's exit is noteworthy in the seemingly concerted approach the operators took to announce and gradually close the shop over an extended 30-day period; they also permitted users to spend their remaining account balances within the shop while it remained open. It can be tempting to give credence to popular rumors regarding the motivations behind the Joker's Stash closure, but it will take more time, if ever, to fully understand and unearth what took place.

Joker's Stash added some final parting words for the carding community:

We are also want to wish all young and mature ones cyber-gangsters not to lose themselves in the pursuit of easy money.

Remember, that even all the money in the world will never make you happy and that all the most truly valuable things in this life are free.

What's Next?

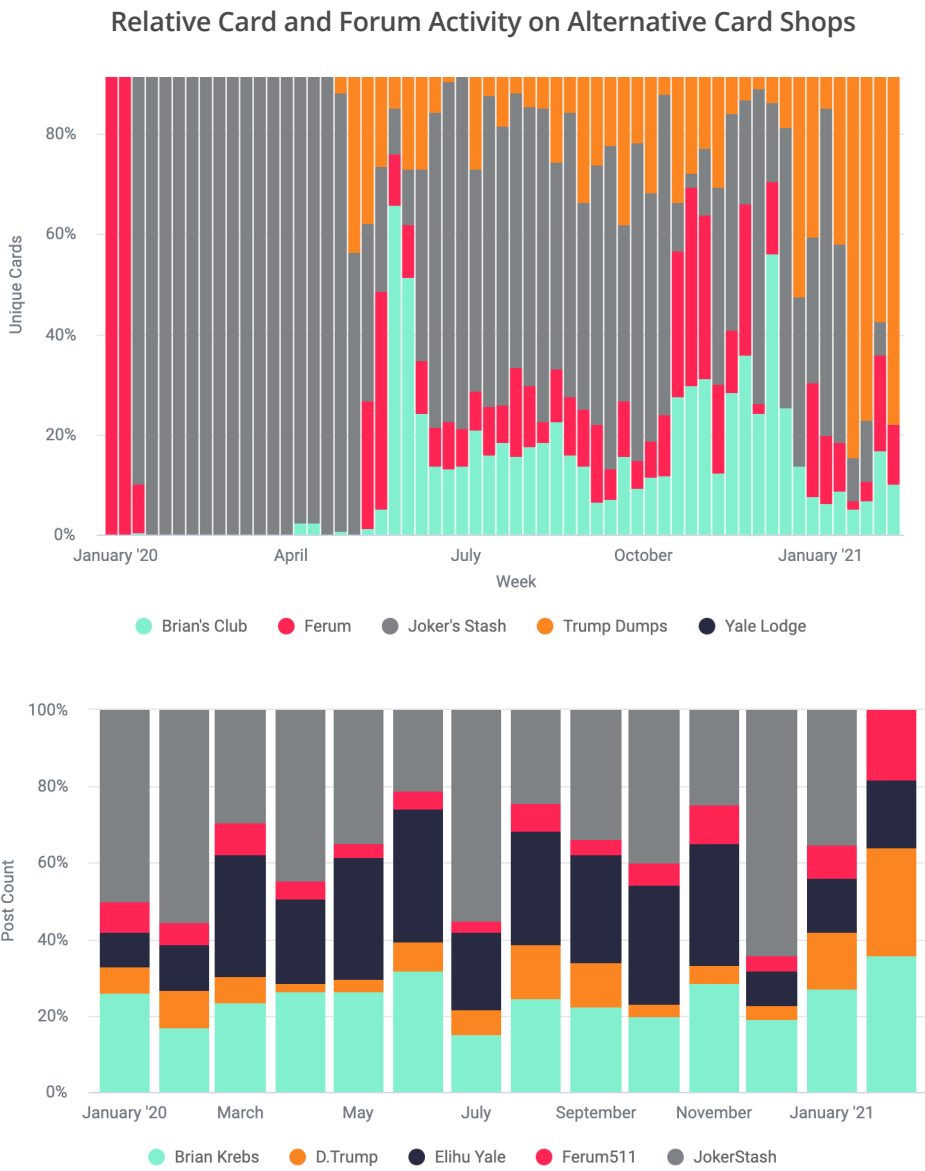
Card fraud, of course, won't stop because Joker's Stash is done. Just as Joker's Stash rose to prominence during a void in competitive illicit marketplaces, we expect new and existing shops to try to swoop in and fill the gap left by Joker's Stash.

Four Card Shops Are Primed to Replace Joker's Stash

Flashpoint continues to track all of the relevant cybercriminal forums, communities, and carding shops (see Figure 3). Based on our current understanding of the market and recent chatter that we've analyzed, we see four shops as the most-relevant and most-likely marketplaces to take over (listed alphabetically):

1 Brian's Club: Since news of Joker's Stash closing, Brian's Club has significantly increased their advertisements on carding forums and chat rooms in an attempt to attract new users. It offers a high amount of support on various forums and has fully recovered from the breach that took down the shop back in October of 2019.

- 2 Ferum:** The administrator of Ferum maintains a long-standing presence in carding communities. The shop is available on clear web and Tor, providing easier access for entry-level cybercriminals. However, the relatively low amount of card content has limited broader scale adoption.
- 3 Trump's Dumps:** A relatively newer shop, it too has increased advertisements to capture the open market share left in Joker's Stash absence. The shop offers a variety of services, including a self-hosted checker within the shop.
- 4 Yale Lodge:** A Tor and clear web card shop with a relatively high degree of customer support, as well as a self-hosted checking service.



Evaluating the Alternatives

When reviewing the Joker’s Stash replacement candidates, there are several factors to consider (see Figure 4). It can be tempting to focus on shop activity and transaction volume to predict the next shop to lead the market. However, if that’s your only evaluator, you overlook quality elements of many, often more important, card shop attributes that sellers and buyers will consciously and unconsciously take into consideration, including:

- 1 Self-hosted checker services:** Credit card checkers quickly check card validity by attempting small transactions, typically between (USD) \$0.01 and \$0.10. When shops provide self-hosted checkers, they enable customers to quickly and easily assess potential purchases and to receive refunds in cases where proclaimed valid cards are declined.
- 2 Customer support:** The ability of the shop to provide timely support either via their own ticketing system within the shop or on various forums.
- 3 Additional offerings:** Supplemental products and services that can automate or otherwise enhance carding techniques for customers. This can often be tools like SSN-DOB offerings, BIN or ZIP lookups, etc.

- 4 CNP Volume (6 months):** The published volume of CNP card data purchases that were collected from intercepted network traffic.
- 5 CP Volume (6 months):** The amount of CP card data purchases that were skimmed from a physical card via skimmer device or point of sale (POS) malware.
- 6 Forum post volume (6 months):** The number of community posts that were authored by spokespeople associated with their respective shops.
- 7 Activity length (years):** The length of time that the shop, and the threat actors behind it, have been active since first going online.
- 8 Payment method:** The types of cryptocurrencies that are acceptable forms of payment on the shop.
- 9 Network infrastructure:** The locations and networking infrastructure leveraged for the shop to operate. Depending on the available options, they connote the relative ease of use, safety, privacy, and security of shop access, communications, and transactions.

Shop Name	Brian's Club	Ferum	Joker's Stash	Trump's Dumps	Yale Lodge
Self Hosted Checker Service	Yes	No	Yes	Yes	Yes
Customer Support	Yes	Yes	Yes	Yes	Yes
Additional Product Offerings	Yes	No	Yes	No	Yes
CNP Vol. (6 months)	400K	2M	2M	83K	83K
CP Vol. (6 months)	2.3M	0	6.1M	5M	0
Forum Post Vol. (12 months)	1,000	240	1,800	300	1,000
Forum Activity Length (years)	8	10	7	4	6
Payment Methods	BTC, LTC, Dash	BTC	BTC, LTC, Dash	BTC	BTC
Network Infrastructure	Tor + clear web	Tor + clear web	Blockchain DNS + clear web	Tor	Tor + clear web

Brian's Club Appears Well-Positioned as the Next Top Shop

Based on the above criteria and our qualitative analysis of current carding community trends and conversations, Brian's Club seems to be the lead candidate as the shop to pick up the mantle from Joker's Stash. Brian's Club's balanced mix of high-quality cards and dumps, respectable CP and CNP volume, and 8-year-long tenure on the market will give cybercriminals relative ease in conducting their illicit business through the marketplace.

Even with all of this in consideration, Brian's Club is far from a sure thing. And even if it does take the top spot in the market, it will still have to make up considerable ground to come close to rivaling Joker's Stash at its peak.

How Will Card Fraud Evolve?

When Joker's Stash launched in 2014, carders were staring over a cliff as the October 2015 EMV liability shift was soon to take effect. This mandate—which emerged in the aftermath of the aforementioned large card breaches at major retailers—holds merchants responsible for

transaction losses resulting from failure to implement chip-and-pin card protections.

Carders' initial fears of the implications of the EMV liability shift, however, turned out to be overblown. The implementation of chip-and-pin has been **remarkably slow in the US** and is only now in 2021, beginning to reach mass levels of adoption.

Chip-and-Pin Is Finally Beginning to Disrupt Card Fraud Markets

Joker's Stash's success can, at least in part, be attributed to correctly anticipating (or luckily disregarding) the slow chip-and-pin adoption in the US that should have taken hold in late 2015. The remaining card shops won't be so lucky, as the volume of CP data has been noticeably on the decline for the past 12 to 18 months.

The shops that remain in operations today, as well as any new entrants, will need to adjust to these increasingly quick-shifting trends occurring across the payment landscape.

Card Shops Will Take New Forms

Despite the evasive maneuvers of shop administrators (e.g., Tor-hosted infrastructure and blockchain DNS domains), card shops remain compelling targets for law enforcement. To counter enforcement scrutiny, new and smaller shops may transition to new operational models and host their platforms via entirely closed forums and encrypted messaging apps.

As obstacles and shop countertactics continue to escalate, the barrier to entry for new shops will increase as a result. The better quality shops will demand increasingly higher registration fees and become less specialized as they introduce new products and services (e.g., checking services) to boost sales.



Turn Insight into Action with Flashpoint

Schedule a demo with Flashpoint to see where your organization, your assets, and your personnel may be exposed online.

Equipped with organization-specific threat intelligence, leading organizations worldwide use Flashpoint to turn threat intelligence into security action: Lock down compromised accounts, identify insider threats, recover exposed strategic and sensitive data, and more.

CREDITS

Thank you to Flashpoint Contributors, including Ian Gray, Maxwell Aliapoulos, and Vlad Cuiujuclu. A special thanks to the entire Flashpoint Intelligence Analyst team for supporting the research and analysis that made this report possible.

ABOUT FLASHPOINT

Flashpoint is the globally trusted leader in actionable threat intelligence for organizations that demand the fastest, most comprehensive coverage of threatening activity on the internet. From bolstering cyber and physical security, to detecting fraud and insider threats, Flashpoint partners with customers across private and public sectors to help them rapidly identify threats and mitigate their most critical security risks. Flashpoint is backed by Georgian Partners, Greycroft Partners, TechOperators, K2 Intelligence, Jump Capital, Leaders Fund, Bloomberg Beta, and Cisco Investments.

For more information, visit www.flashpoint-intel.com or follow us on Twitter at [@FlashpointIntel](https://twitter.com/FlashpointIntel).