

INCOGNITO MARKET: TRUST AMONG CRIMINALS?

By Maria Leticia Arantes, Oliver Schilke, and Gabriel Rossman

In February 2024, users of Incognito Market—a popular dark web marketplace—began experiencing issues with withdrawing funds, sparking concern among the platform’s vendors and buyers. Incognito Market, managed by a cryptic figure known as “Pharoah,” had built a reputation for security and trust among dark web users, allowing millions of dollars in transactions since its inception in 2020. However, in February, Pharoah restricted withdrawals while still accepting deposits, sparking suspicion of an exit scam. This fear was confirmed when Pharoah posted a ransom demand, threatening to release users’ transaction histories and private messages unless they paid to have their records purged. With identities, reputations, and possibly lives at stake, Pharoah’s announcement placed Incognito’s vendors and customers in a precarious position. They were facing a daunting choice: should they comply with Pharoah’s extortion demands, risking further scams, or refuse to pay, risking exposure? In a high-stakes dilemma where trust is scarce and uncertainty is high, what would you do? Ultimately, can there be real trust among criminals?

Background on the Dark Web

Most internet users browse online content while sticking to the surface web—the visible, accessible part of the internet where search engines can easily find websites. But it turns out that this only makes up a sliver of the total internet—about 5%. Below it lies a hidden world known as the “dark web.”

The story of the dark web begins in 2000 when Ian Clarke, a computer science student at the University of Edinburgh, designed an online space where people could communicate anonymously without censorship for his thesis project, and called it Freenet. Freenet was like opening Pandora’s box, laying the groundwork for what would become one of the most controversial realms of the internet.¹

The U.S. Naval Research Laboratory took Clarke’s thesis project even further in 2002 when they developed The Onion Router, or Tor, for use by U.S. intelligence, allowing agents to communicate secretly over the web. Considering it would be useless to anonymize technology that is known to be used only by one spy agency, the government released it as open-source software in 2004, hoping to make it accessible to anyone who wanted online anonymity.² This led to the creation of the nonprofit Tor Project, with a special “onion routing” technology that adds layers of encryption and bounces users’ data through a maze of random relay points that make it nearly impossible to trace.³

While Tor was a haven for privacy-seekers under repressive regimes, people interested in illegal commerce soon found their way onto this shadowy network. By 2009, the term “dark web” started making headlines, linking the network to hidden criminal activities. In 2011, the dark web made its way into the limelight with the rise of Silk Road, the dark web’s first black market, set up by Ross Ulbricht.⁴ With the advent of Bitcoin, transactions could now happen without leaving

¹ “Everything You Should Know About the Dark Web,” Tulane University School of Professional Advancement, accessed October 2024, <https://sopa.tulane.edu/blog/everything-you-should-know-about-dark-web>

² Adam Volle, “dark web,” Britannica, accessed October 2024, <https://www.britannica.com/technology/computer-security>

³ Ibid 1

⁴ Ibid 2

traceable credit card information, giving illegal trade a new, untraceable currency. Even though the FBI arrested Ulbricht in 2013 and Silk Road was shut down, imitators quickly sprung up and continue to do so today.

Pharoah; The Supreme Ruler

Incognito Market was established in October 2020 by Rui-Siang Lin 林睿庠, 23, of Taiwan. Described in his [GitHub account](#) as a “Backend and Blockchain Engineer, Monero Enthusiast,” Lin is a knowledgeable person in the field of security and cryptocurrency. The approximately 35 articles on cryptocurrency investment, use of blockchain, and software coding in his publicly available GitHub account indicate that Lin has significant computing knowledge and technical prowess.⁵ When he was a high-school student, Lin set up his own Web sites and was known by his peers as a “genius” and an outstanding talent in mathematics.⁶ As Incognito Market’s principal administrator, Lin was anonymously known by the alias “Pharoah.”

Incognito Market facilitated an overall sale of more than \$100 million in its 41 months of operation. In his short career, Pharoah built Incognito into a popular crypto black market with some of the dark web’s better safety and security features.⁷ Its popularity can be gauged from the fact that by June 2023 it was generating sales of \$5 million per month.⁸ Transactions on this marketplace were conducted exclusively through cryptocurrencies, such as Bitcoin or Monero, requiring users to transfer funds from their individual digital wallets to a designated wallet created by the Incognito Market at the time of registration and integrated within the platform’s infrastructure.⁹ In the market, purchasing goods involved transferring funds from the buyer’s wallet to the seller’s wallet within the Incognito Market. Sellers then withdrew their earnings to their personal cryptocurrency wallets.

Trust on the Dark Web

But how could a platform on the darknet run by an anonymous entity with questionable motives and frequented by criminals create the trust needed for buyers to transfer large sums of money to unknown strangers without having legal recourse in case something goes wrong? Both extraordinary uncertainty and complete lack of protection by a legal system make considerable trust necessary for an illicit marketplace to work.¹⁰ On Incognito, this level of trust was produced by design. Several mechanisms created trust in the vendors on the platform as well as the platform itself.

⁵ Mihir Bagwe, ““Incognito Market” Operator Arrested for Running \$100M Narcotics Marketplace,” The Cyber Express, May 21, 2024, <https://thecyberexpress.com/incognito-market-operator-arrested/>

⁶ Jason Pan, “People who knew alleged ‘Pharoah’ of online drugs site surprised at arrest”, Taipei Times, May 23, 2024, <https://www.taipeitimes.com/News/taiwan/archives/2024/05/23/2003818282>

⁷ Andy Greenberg, “He Trained Cops to Fight Crypto Crime—and Allegedly Ran a \$100M Dark-Web Drug Market”, Wired, May 23, 2024, <https://www.wired.com/story/lin-rui-siang-incognito-market/>

⁸ ““Incognito Market” Owner Arrested for Operating One of the Largest Illegal Narcotics Marketplaces on the Internet,” Office of Public Affairs – US Department of Justice, May 20, 2024, <https://www.justice.gov/opa/pr/incognito-market-owner-arrested-operating-one-largest-illegal-narcotics-marketplace>

⁹ See Exhibit 1 for the bank’s graphic interface.

¹⁰ Robert A. Hardy, Julia R. Norgaard, “Reputation in the Internet Black Market: An Empirical and Theoretical Analysis of the Deep Web,” *Journal of Institutional Economics* 12, no. 3 (2016): 515–39, <https://doi.org/10.1017/S1744137415000454>.

To promote buyer trust in vendors, the Incognito Market used an escrow system, such that the marketplace held the payment until the buyer confirmed receipt of the product. This helped ensure that the seller delivered the product before receiving the payment.¹¹ Moreover, the platform had a reputation system, on which buyers could rate and review sellers based on their experiences. This system helped build trust, as buyers could assess the history and reliability of sellers through their ratings and reviews.¹² And not everyone could simply offer goods and services on the platform; the Incognito Market required vendors to undergo a verification process before they could start selling. This process often involved providing proof of identity or paying a deposit, which added a layer of security and accountability to the transactions.¹³ Perhaps most importantly, the Incognito Market used the Tor network for browsing, which helped maintain user pseudonymity and security. This made it difficult for law enforcement to trace transactions, allowing criminal activities to remain undetected.¹⁴

In addition to creating trust in vendors, Incognito was also successful in creating system trust in the platform itself.¹⁵ It featured a well-designed, user-friendly interface similar to legitimate e-commerce sites. This included easy navigation, a search function, and clear product listings, which made the buying process straightforward and conveyed a trustworthy feel to users.¹⁶ One of the most intriguing aspects of the Incognito Market was its vibrant community. Users actively engaged in forums to discuss their experiences, share tips, and warn each other about potential scams. This open communication fostered a sense of solidarity and transparency, which was essential for maintaining trust in such a high-risk environment. The culture of the marketplace was one of cautious collaboration, where users balanced trust and suspicion. Further, the Incognito Market had mechanisms in place for resolving disputes between buyers and sellers, ensuring that issues could be addressed efficiently. Finally, Incognito's reputation benefitted from the longevity and scale of the platform, handling over \$100 million in transactions.¹⁷

A Look into Pharaoh's Exit Scam

On February 19th, 2024, Incognito Market largely disabled crypto withdrawals, with the CAPTCHA tool ceasing to function. However, deposits were still possible. Consequently, users went on different social media platforms like Reddit and X with accusations. Pharaoh responded with a post on Dread, a forum similar to Reddit, blaming these issues on recent system updates and promising they would soon be resolved: "Please note that the initial stages of this update may briefly impact usability in the first few days as the servers perform multiple tasks both when syncing old data and new requests."¹⁸

¹¹ "Incognito market," Github, February 2024, <https://github.com/vpx62rks/Incognito-market>

¹² Paulina Elizabeth, "The Incognito Market Reddit: Unveiling the Anonymous World of Online Commerce," Medium, Oct 9, 2023, <https://medium.com/@adryfgznzz/the-incognito-market-reddit-unveiling-the-anonymous-world-of-online-commerce-a02ee28b4980>

¹³ See Exhibit 1 for the bank's graphic interface.

¹⁴ Erinn Clark, Linus Nordberg, "The Tor Project Anonymity Online", accessed July 2024, <https://media.torproject.org/outreach-material/presentations/FSCONS-2010/FSCONS-2010.pdf>

¹⁵ Marcos Aguiar, Jeff Kiderman, Harsha C. Shekar, Oliver Schilke, "Safeguarding trust in a digital ecosystem," *Journal of Business Strategy*, (2023), <https://doi.org/10.1108/JBS-08-2023-0157>.

¹⁶ See Exhibit 1 for the bank's graphic interface.

¹⁷ Rhodilee J. Dolor, "Feds Arrest Owner of \$100,000,000 Dark Web Marketplace Using Crypto To Process Drug Transactions," The Daily Hodl, May 27, 2024, <https://dailyhodl.com/2024/05/27/feds-arrest-owner-of-100000000-dark-web-marketplace-using-crypto-to-process-drug-transactions/>

¹⁸ See Exhibit 2.

Nevertheless, ongoing user reports regarding difficulties in withdrawing funds persisted, subsequently validated by a statement from the administrator of Dread, labeling the situation as an "exit scam." Posted by the user *Hugbunt3r*, the statement detailed a conversation with Pharaoh, during which *Hugbunt3r* was allegedly offered a "bribe" to delete any Dread forum posts related to the Incognito Market. He also advised users to avoid depositing funds into the marketplace.¹⁹

An exit scam refers to a deceptive tactic whereby a company or venture abruptly shuts down, with its operators vanishing, along with the funds belonging to users or investors. This scenario is not infrequent within the realm of cryptocurrency and financial endeavors, particularly on darknet platforms and markets where users engage in the trading of illicit goods.²⁰

When the Exit Scam Became an Extortion Scam

Unlike previous dark web exit scams, Incognito Market did not take down the website after appropriating user funds. The homepage for the Incognito Market was updated to include a blackmail message from its owners, threatening to publish cryptocurrency transactions and chat records of users who refused to pay a ransom to keep the records confidential.

"We got one final little nasty surprise for y'all," read the message to Incognito Market users. "We have accumulated a list of private messages, transaction info and order details over the years. You'll be surprised at the number of people that relied on our 'auto-encrypt' functionality. And by the way, your messages and transaction IDs were never actually deleted after the 'expiry'....SURPRISE SURPRISE!!! Anyway, if anything were to leak to law enforcement, I guess nobody never slipped up."²¹

When engaging in transactions on the dark web, it is customary to employ encryption protocols such as PGP to secure communications. Users generate personal "private" and "public" encryption keys and circulate the public keys so partners can encrypt messages that can only be decrypted by the private key. Utilizing these keys preserves privacy and verifies identity. However, many users of the Incognito Market relied heavily on its auto-encryption feature, which allowed Pharaoh to preserve private keys and thereby decrypt messages. Thus, records including messages and transaction IDs, which were intended to have a limited lifespan, remained preserved within the marketplace's database indefinitely.

In response to these revelations, Pharaoh announced his intention to disclose a comprehensive data dump comprising 557,000 orders and 862,000 cryptocurrency transaction IDs by the conclusion of May. "We'll be publishing the entire dump of 557k orders and 862k crypto transaction IDs at the end of May, whether or not you and your customers' info is on that list is totally up to you." Pharaoh. "And yes, this is an extortion!!!!"²²

Pharaoh had priced the extortion based on vendors' status or "level" within the marketplace. Level 1 vendors could have their information removed by paying a \$100 fee. However, larger "Level 5" vendors were asked to cough up \$20,000 payments.²³ By clicking a button that said "Purge Records", users could make an official transaction.²⁴ The extortion message also included a "Payment Status" page that listed the darknet market's top vendors by their handles,

¹⁹ See Exhibit 3.

²⁰ "Crypto Glossary/Exit Scam," COIN360, accessed August 2024, <https://coin360.com/glossary/exit-scam>.

²¹ See Exhibit 4.

²² See Exhibit 4.

²³ See Exhibit 5.

²⁴ See Exhibit 5.

saying at the top that “you can see which vendors care about their customers below.”²⁵ The names in green supposedly corresponded to users who opted to pay.

The exit scam occurred during a boom in the price of Bitcoin, when the cryptocurrency reached its then record high of \$68,990, setting a new peak just above \$69,200. Of course, the higher the Bitcoin value, the higher the amount of stolen funds.²⁶

Even though vendors were targeted first, customers of Incognito did not escape the extortion attempts, as Pharaoh left a message for them too: “As for the buyers, we’ll be opening up a whitelist portal for them to remove their records as well in a few weeks.”²⁷ However, this ‘service’ came at a price, with the admin noting that prices will double on April 1st, coinciding with when buyers could access the page to get their names whitelisted.²⁸

What Would You Do?

For Incognito Market users—especially vendors whose business reputations and personal safety were at stake—the dilemma went beyond financial loss. After Pharaoh’s announcement of the ransom, users faced a troubling choice: Should they pay, trusting that Pharaoh, an anonymous figure who had created an illegal marketplace, would honor his word and delete their information? Or should they refuse, risking exposure that could reveal their identities and illegal activities to both law enforcement and the darknet community? This decision forced users to consider whether they could trust a criminal whose actions were already unpredictable and self-serving. Would paying the ransom buy protection, or would it simply make them more vulnerable to future extortion schemes? In the face of an uncertain outcome and high stakes, what would you do if your reputation and identity hung in the balance and whether to trust or not to trust a criminal was your last resource?

April Fools!

When when April 1st finally came, Pharaoh claimed it was all an April Fool’s joke, suggesting all data had been deleted as promised.²⁹ This meant that all vendors were robbed and those who rushed to pay the admin were also scammed.

Pharaoh’s erratic actions and multiple scams made it difficult for market participants to trust him. The mix of fear and a misplaced sense of duty to protect customer data led some vendors to pay the ransom, revealing a complex web of ethics and desperation within the darknet marketplace.

The Bigger Picture

The Incognito Market highlights significant ethical and economic challenges. For law enforcement, these platforms represent a formidable challenge, requiring sophisticated strategies to infiltrate and dismantle. For users, the case underscores the risks inherent in engaging with anonymous, unregulated marketplaces. At the same time, Incognito offers a window into an extreme case of trust production and betrayal that also offers important lessons for the design of legitimate marketplaces.

²⁵ See Exhibit 6.

²⁶ “TOP 2 Darknet marketplace was suspected of being a scam. Is it surprising?,” AMLCrypto, accessed Jul 20, 2024, https://amlcrypto.io/blog/thetop_2_darnet_marketplace_was_suspected_of_being_a_scam

²⁷ See Exhibit 4.

²⁸ See Exhibit 5.

²⁹ See Exhibit 7.

Exhibits

Exhibit 1: Incognito Market Cryptocurrency Transfer Interface



Source: “‘Incognito Market’ Owner Arrested for Operating One of the Largest Illegal Narcotics Marketplaces on the Internet,” Office of Public Affairs – US Department of Justice, May 20, 2024, <https://www.justice.gov/opa/pr/incognito-market-owner-arrested-operating-one-largest-illegal-narcotics-marketplaces>

Exhibit 2: Pharaoh's Posts Updates on Dread



Dark Web Informer   @DarkWebInformer

pharoah from Incognito Market has provided the following in regards to BTC and XMR issues. [#Incognito](#) [#IncognitoMarket](#) [#DarkWebInformer](#) [#Cybersecurity](#) [#Cyberattack](#) [#Cybercrime](#) [#Darknet](#)

Atomic Withdrawal Wallets Online 

by /u/pharoah  • 6 minutes ago* in /d/IncognitoMarket

We have made changes to our withdrawal systems, crypto wallets are now running as multiple clustered servers instead of a centralized wallet. We hope that by increasing the capacity of throughput, we can handle much heavier withdrawal and deposit demand, while preparing for the launch of stablecoin and Ethereum integration.

Please note that the initial stages of this upgrade may briefly affect usability in the first few days since the servers are multitasking on both old data synchronization and new requests.

And to keep it as transparent as always in light of the ever-existing FUDs, there are currently 154 withdrawals both BTC and XMR that are in queue for processing, which is approximately 3% of total number of withdrawals submitted in the last 24 hours. Please bear with us for a moment, the coins will arrive, as they always do and always have been.

Our team aims to launch the major interface and currency upgrade before our three year anniversary.

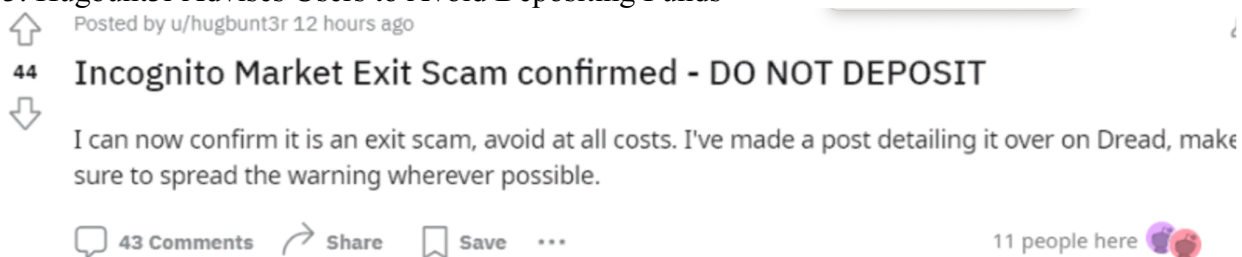
Cheers,
pharoah


@DarkWebInformer

1 comments


Source: "TOP 2 Darknet marketplace was suspected of being a scam. Is it surprising?," AMLCrypto, accessed Jul 20, 2024, https://amlcrypto.io/blog/thetop_2_darnet_marketplace_was_suspected_of_being_a_scam




Exhibit 3: Hugbunt3r Advises Users to Avoid Depositing Funds





 Posted by u/hugbunt3r 12 hours ago

44 **Incognito Market Exit Scam confirmed - DO NOT DEPOSIT**

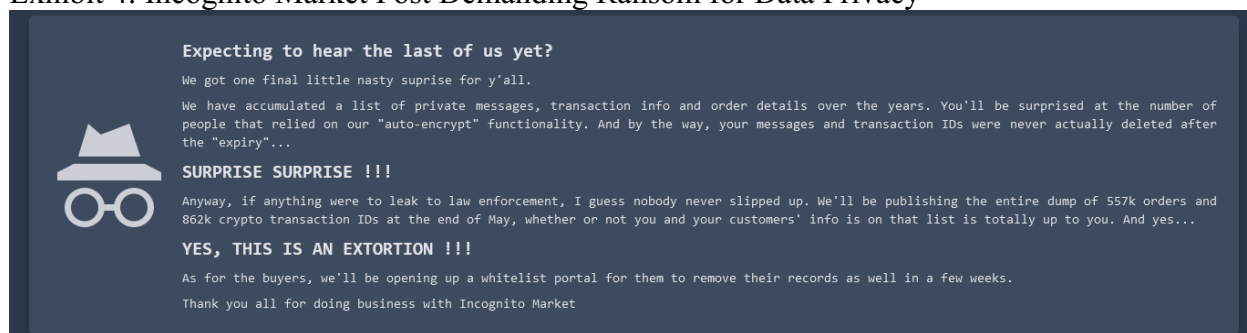
 I can now confirm it is an exit scam, avoid at all costs. I've made a post detailing it over on Dread, make sure to spread the warning wherever possible.

 43 Comments  Share  Save ...

11 people here  

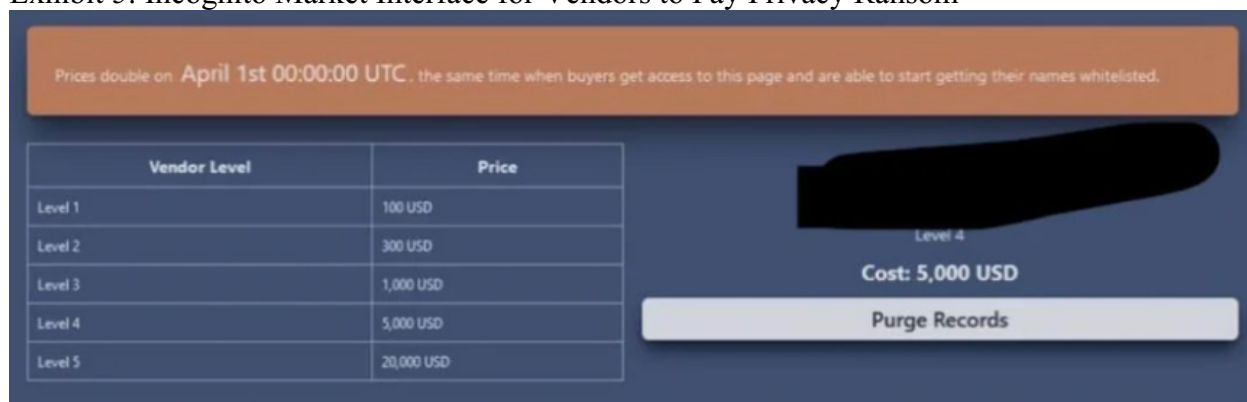
Source: "TOP 2 Darknet marketplace was suspected of being a scam. Is it surprising?," AMLCrypto, accessed Jul 20, 2024, https://amlcrypto.io/blog/thetop_2_darnet_marketplace_was_suspected_of_being_a_scam

Exhibit 4: Incognito Market Post Demanding Ransom for Data Privacy



Source: "Incognito Darknet Market Mass-Extorts Buyers, Sellers," Krebs on Security, March 11, 2024, <https://krebsonsecurity.com/2024/03/incognito-darknet-market-mass-extorts-buyers-sellers/>

Exhibit 5: Incognito Market Interface for Vendors to Pay Privacy Ransom



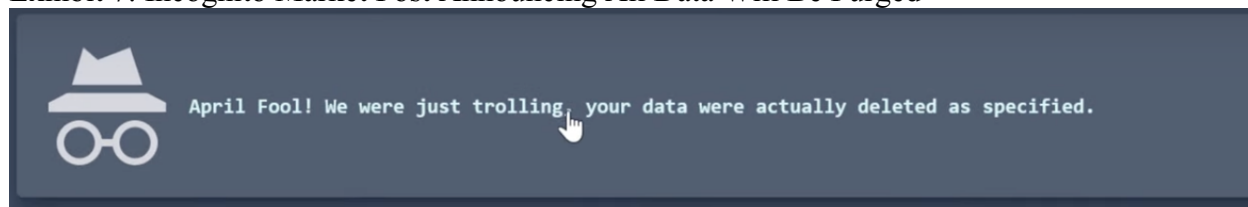
Source: "Incognito Darknet Market Mass-Extorts Buyers, Sellers," Krebs on Security, March 11, 2024, <https://krebsonsecurity.com/2024/03/incognito-darknet-market-mass-extorts-buyers-sellers/>

Exhibit 6: Incognito Market Post Listing Which Vendors Had Paid Privacy Ransoms

Payment Status					
You can see which vendors care about their customers below					
OliViA12	0zr0rt	14bdoking	1box2box	1hero	1stopquickshop
1STOPSHOP	200198	321SNORT	3APES	420Services	4wardnkcab
4WheelsPharma	54Aunt	5starhaze	777lucky	7Eleven	8drugsafe
99CentStore	aactiveshooter	A8Grade	abit	abLoneLSD	AbsolutBuds
acelabsofficial	acdbern	Acassallstars	ActiveJ	AddamsFamily	AdderallCanada
adderallzthe2nd	addyexpress	addygawd	addyrus	AddyShope	ADHD
agentxorders	airdnd	Ajexamsterdam	akgenericss	AladinXpress	albeagle
alfa	allADDYallRX	allbest01	AllDRUGZ	allelements	ALLinDRUGS
ALLREALPILLS	AllThingsCanna	AlPacino	Alphafakes	alphapatriot1	alroundmarketNL
alwaysfire	amazedals42	AmazonCrime	AmazonDelivery	amazonprime	amazonprimeUK
AmazonRX	AmazonUK	ambassador	Amer1canSpint	AmericanSteroid	americansteroids
AmphetamineCowboys	AmsterdamFinest	amsterdamonline	ananasexpress	AngieValencia	annieadderall
anonqwertz	anonsheep	anonyms	Antia77	AotearoaOCM	ApexBear
ApexSupplies1	ApocalypseLabs	apricots	apronsmash	arakar	arbha
Area420	artzduyasi	ASAPWINTER	Asclearascrystal	AshWilliams	Asmodeuss
ATHCNM	AthKKSP	ATLASGROUP24	atomics	AusFun	Auslab84
ausmdma	ausmeds	ausmedz	ausnarcoslord	auspride	aussiedank
aussiedank1	AussieDMT	aussieempireee	aussiehits	AussieMD22	aussieme

Source: "Incognito Darknet Market Mass-Extorts Buyers, Sellers," Krebs on Security, March 11, 2024, <https://krebsonsecurity.com/2024/03/incognito-darknet-market-mass-extorts-buyers-sellers/>

Exhibit 7: Incognito Market Post Announcing All Data Will Be Purged



Source: "Incognito Darknet Market's 'April Fool' Message," Apr 2, 2024, YouTube video, 9:47, <https://youtu.be/tTDZi00bdNY?si=hQVsGJpAG2c-8RtF>