CONSUMER FINANCIAL PROTECTION BUREAU | NOVEMBER 2022

Complaint Bulletin

An analysis of consumer complaints related to crypto-assets

Consumer Financial Protection Bureau

Table of contents

Executive summary

Crypto-assets are increasingly offered and marketed to consumers, including being incorporated into other products such as credit, debit, and prepaid cards offering rewards in crypto-assets, crypto-asset product offerings by person-to-person (P2P) payments platforms. Even large financial firms have begun offering and marketing crypto-asset custodial services to certain customers. As these offerings have increased, so too have consumers' complaints to the Consumer Financial Protection Bureau (CFPB) related to crypto-assets.

The majority of the more than 8,300 complaints related to crypto-assets submitted to the CFPB from October 2018 to September 2022 have been submitted in the last two years with the greatest number of complaints coming from consumers in California. In these complaints, the most common issue selected was fraud and scams (40%), followed by transaction issues (with 25% about the issue of "Other transaction problem," 16% about "Money was not available when promised," and 12% about "Other service problem"). In addition, analyses suggest that complaints related to crypto-assets may increase when the price of Bitcoin and other crypto-assets increase.

This report finds that fraud, theft, hacks, and scams are a significant problem in crypto-asset markets:

- **The top issue across all crypto-asset complaints was "Fraud or scam."** This issue appears to be getting worse, as fraud and scams make up more than half of "virtual currency" complaints received thus far in 2022. Some consumers stated that they have lost hundreds of thousands of dollars due to unauthorized account access. The prevalence of fraud and scam complaints raises the question of whether crypto-asset platforms are effectively identifying and stopping fraudulent transactions.
- **Consumers report many different scam types, including romance scams, "pig butchering," and scammers posing as influencers or customer service.** Crypto-assets are often targeted in romance scams, where scammers play on a victim's emotions to extract money. According to the FTC, of all romance scam payment types, crypto-asset romance scams accounted for the highest median individual reported losses

at $10,000.[1] Some of these scammers employ a technique law enforcement refers to as "pig butchering," where fraudsters pose as financial successes and spend time gaining the victim's confidence and trust, coaching victims through setting up crypto-asset accounts.[2] Some scammers try to use social media posts by crypto-asset influencers and celebrities to trick victims. Finally, lack of customer service options for many crypto-asset platforms and wallets creates opportunities for social media scams where attackers pretend to be customer service representatives to gain access to customers' wallets and steal crypto-assets.

- **Crypto-assets are a common target for hacking.** Consumers reported "SIM-swap" hacks, where an attacker intercepts SMS messages to exploit two-factor authentication, and phishing attacks, social engineering, or both. Companies often responded to these complaints by stating that consumers are responsible for the security of their accounts. Crypto platforms are a frequent target of hacks by malicious actors, including certain nation-state actors. Hackers affiliated with one nation state have stolen over $2 billion in crypto-assets total[3], including more than $1 billion from Jan 2022 – July 2022 alone[4], and their hacks have included several prominent crypto platforms, including a "play to earn" crypto-asset game.[5]

- **There are signs that older consumers are also impacted by crypto-asset frauds and scams.** Older consumers report a higher rate of crypto-asset related frauds and scams compared to complaints overall: 44% versus 40%.

- **Complaints suggest that servicemembers are facing issues with crypto-asset scams.** Servicemembers have submitted complaints about "SIM-swap" hacks, identity

---

[1] Fed. Trade Comm'n, Data Spotlight: Reports show scammers cashing in on crypto craze (June 2022), http://www.ftc.gov/system/files/ftc_gov/pdf/Crypto%20Spotlight%20FINAL%20June%202022.pdf.

[2] *See* FBI Miami Field Office and the Internet Crime Complaint Center (IC3), *Cryptocurrency Investment Schemes* (Oct. 3, 2022), https://www.ic3.gov/Media/Y2022/PSA221003.

[3] *See, e.g.,* Elliptic Connect, The $100 Million Horizon Hack: Following the Trail Through Tornado Cash to North Korea (June 6, 2022), https://hub.elliptic.co/analysis/the-100-million-horizon-hack-following-the-trail-through-tornado-cash-to-north-korea/.

[4] *See, e.g.,* Choe Sang-Hun and David Yaffe-Bellany, *How North Korea Used Crypto to Hack Its Way Through the Pandemic*, NYTimes (Jul. 2022), https://www.nytimes.com/2022/06/30/business/north-korea-crypto-hack.html.

[5] *See* Statement, Fed. Bureau of Investigation, *FBI Statement on Attribution of Malicious Cyber Activity Posed by the Democratic People's Republic of Korea* (Apr. 14, 2022), https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea. *See also* Aaron Schaffer, *North Korean hackers linked to $620 million Axie Infinity crypto heist*, Washington Post (Apr. 14, 2022), https://www.washingtonpost.com/technology/2022/04/14/us-links-axie-crypto-heist-north-korea/.

theft, and romance scams. Servicemembers have also submitted complaints about transaction problems and poor customer service at crypto-asset platforms.

- **Complaints about frauds or scams continue to rise, making up more than half of all total crypto-asset complaints received by the CFPB thus far in 2022.** Crypto-asset complaints and fraud reports have also been increasing at other federal agencies: The SEC has received over 23,000 tips, complaints, and referrals regarding crypto-assets since fiscal year 2019, with a particularly sharp increase in the last two years,[6] while crypto-asset losses reported to the FTC in 2021 were nearly sixty times more than in 2018.[7]

Consumer complaints describe a wide range of account access and dispute resolution issues, including platform bankruptcies where their assets are indefinitely frozen, weeks-long waits due to account access problems, hours-long platform outages, difficulty executing transactions, and poor customer service.

- **Frozen accounts, platform bankruptcies, and consumer losses.** Several large crypto-asset platforms have recently either frozen customers' account withdrawals, filed for bankruptcy protection, or both. These failures have impacted millions of consumers.[8] The CFPB has received several complaints about crypto-asset platforms that froze consumers' assets before filing for bankruptcy protection. Some consumers report losing six figures or more due to the platform's failures. Consumers describe companies that misled them, refused or ignored requests to withdraw the U.S. dollars consumers deposited with these platforms, and contradicted their disclosures. Similar claims have been raised in letters filed in certain crypto-asset bankruptcy proceedings.[9]

---

[6] Fin. Stability Oversight Council, Report on Digital Asset Financial Stability Risks and Regulation (Oct 3, 2022), https://home.treasury.gov/system/files/261/FSOC-Digital-Assets-Report-2022.pdf ("FSOC Report on Digital Assets").

[7] Fed. Trade Comm'n, *supra* note 1.

[8] *See, e.g.,* Cision PR Newswire, *Voyager Digital Reports Revenue Of US$102.7 Million For The Quarter Ended March 31, 2022* (May 16, 2022), https://www.prnewswire.com/news-releases/voyager-digital-reports-revenue-of-us102-7-million-for-the-quarter-ended-march-31--2022--301547719.html ("Total funded accounts reached 1,190,000 as of March 31, 2022") *See also* Vicky Ge Huang, *Big Crypto Lender Celsius Freezes All Account Withdrawals*, Wall Street Journal (June 13, 2022), https://www.wsj.com/articles/big-crypto-lender-celsius-freezes-all-account-withdrawals-11655096584; Vicky Ge Huang, *Crypto Broker Voyager Digital Suspends Withdrawals*, Wall Street Journal (July 1, 2022), https://www.wsj.com/articles/crypto-broker-voyager-digital-suspends-withdrawals-11656705822.

[9] Excerpts from letters to the judge in the Voyager Digital bankruptcy case, MollyWhite.com (July 23, 2022), https://blog.mollywhite.net/voyager-letters/; Excerpts from letters to the judge in the Celsius Network bankruptcy case, MollyWhite.com (July 22, 2022), https://blog.mollywhite.net/celsius-letters/.

- **Consumers report difficulty obtaining restitution for hacks or frauds.** In situations where consumers had assets stolen or their account hacked, they are often told there is nowhere to turn for help. Consumers reported losing their life savings in a scam, while the companies stated their assets were not recoverable.

- **Poor customer service is a recurring issue in complaints about crypto-assets.** Consumers described hard to reach, non-responsive, or non-existent customer service. Some consumers reported being unable to get their problem resolved because they cannot reach a human at the company, and that the failure to provide timely customer service exposed them to unnecessary risks.

Consumers also submitted complaints about a series of other issues, including problems with crypto-asset credit, prepaid, and debit cards, unexpected fees or hidden costs, and platforms trying to hide behind terms and conditions.

- **Consumers reported a range of issues with products that have been marketed to them as crypto-asset credit, prepaid, and debit cards.** Consumers reported problems including the inability to make purchases, issues closing their account, rejecting their claims for reimbursement on fraudulent charges, or failing to receive advertised rewards.

- **Undisclosed or unexpected fees costs.** Some consumers complained about undisclosed or unexpected costs on crypto-asset platforms, or claims there were no fees when, in reality, the consumer noticed a large difference between the price the crypto-asset could be purchased and the price it could be sold (the "spread").

1. Introduction

The term "crypto-assets" describes various digital financial assets and their associated products and services, and is the term used in several reports published in response to President Biden's Executive Order on Ensuring Responsible Development of Digital Assets.[10] In its narrowest sense, the term crypto-asset refers specifically to a private sector digital asset that depends primarily on cryptography and a distributed ledger (such as a blockchain) or similar technology.[11] The term "digital assets" refers to two categories of products: central bank digital currencies (CBDCs) and crypto-assets.[12] Other alternative terms to crypto-assets—such as "virtual currencies," "cryptocurrencies," "crypto tokens," "crypto coins," or simply "crypto"—are often used by market participants as a catch-all to describe these assets. These assets can be purchased, sold, loaned, borrowed, stored, sent, and received via accounts and/or digital wallets on crypto-asset platforms or services, though platforms typically require first funding these accounts through a connection to a bank or a purchase from a credit card (which may be facilitated by a third-party payment provider).

Crypto-assets can and often experience significant volatility. For example, in the last year, Bitcoin is down more than 70% as of October 3, 2022, from its November 2021 high, and the market value of all crypto-assets have fallen by as much as 68% as of July 2022.[13]

Crypto-assets can be stored via accounts, digital wallets, or both. Wallets can either be custodied with a crypto-asset platform or service or kept in a software or hardware wallet (on a device such as a USB drive) that is sometimes referred to as "unhosted" wallets.

---

[10] *See, e.g.,* FSOC Report on Digital Assets, *supra* note 6. *See also* U.S. Dep't of the Treasury, Crypto-Assets: Implications for Consumers, Investors, and Businesses (Sept. 2022), https://home.treasury.gov/system/files/136/CryptoAsset_EO5.pdf.

[11] FSOC Report on Digital Assets, *supra* note 6.

[12] *Id.*

[13] *See, e.g.,* Yahoo Finance, Bitcoin USD (BTC-USD), https://finance.yahoo.com/quote/BTC-USD/ (last visited Oct. 3, 2022). *See also* Olga Kharif, *Why Another 'Crypto Winter' Is Test for Digital Money*, Bloomberg (July 27, 2022), https://www.bloomberg.com/news/articles/2022-07-27/why-another-crypto-winter-is-test-for-digital-money-quicktake.

Over the past decade, the sheer number of crypto-assets has vastly expanded. One estimate puts the count of total crypto-assets at more than 1.8 million.[14] A non-trivial percentage of all outstanding crypto-asset tokens are estimated to be scams (such as tokens where a so-called "rug pull" has occurred[15], or tokens explicitly coded to be able to be purchased, but not sold[16]). Nearly all these tokens are available (or at one point were available) on the so-called "decentralized finance" or "DeFi" part of the crypto-asset ecosystem. While there is no generally accepted definition of "DeFi," or what makes a product, service, arrangement or activity "decentralized,"[17] DeFi commonly refers to the provision of financial products, services, and arrangements that use systems built on top of public permissionless blockchains,[18] smart contracts, software applications, and end-user applications, such as web interfaces, which simplify interacting with blockchains.[19]

Once tokens become sufficiently popular on DeFi and/or attract sufficient liquidity, some are listed on large crypto-asset platforms. Estimates of the number of individual crypto-assets available on large crypto-asset platforms range from 16,000[20] to more than 20,000.[21] This

[14] Token Sniffer, https://tokensniffer.com (last visited Nov. 3, 2022).

[15] FSOC Report on Digital Assets, *supra* note 6 at 32.

[16] Chris Stokel-Walker, *How a Squid Game Crypto Scam Got Away With Millions*, Wired (Nov. 2, 2021), https://www.wired.com/story/squid-game-coin-crypto-scam/.

[17] The Bd. of the Int'l Org. of Sec. Comm'n, IOSCO Decentralized Finance Report (Mar. 2022), https://www.iosco.org/library/pubdocs/pdf/IOSCOPD699.pdf.

[18] NIST describes a blockchain as a distributed digital ledger of cryptographically-signed transactions that are grouped into blocks. Each block is cryptographically linked to the previous one (making it tamper evident) after validation and undergoing a consensus decision. As new blocks are added, older blocks become more difficult to modify (creating tamper resistance). New blocks are replicated across copies of the ledger within the network, and any conflicts are resolved automatically using established rules. *See* Nat'l Inst. of Standards and Tech., Blockchain Technology Overview (Oct. 2018), https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8202.pdf.

[19] The Bd. of the Int'l Org. of Sec. Comm'n, *supra* note 17 at 1 ("DeFi products, services, arrangements and activities rely upon systems built on top of public permissionless smart contract platforms, such as the Ethereum blockchain. DeFi involves a multi-layered technology "stack." In summary, at the base, or settlement layer, is the underlying blockchain. On top of the settlement layer, multiple systems of smart contracts (and auxiliary software) create financial products and services (protocols)...these smart contract and software applications may include, among others, activities that are or are akin to offering, trading, lending, borrowing, and asset management activities. End-user applications, such as web interfaces, are built on top of the smart contract layer. Often, end-user applications may aggregate multiple protocols to provide access and interoperability.")

[20] Susannah Hammond and Todd Ehret, *Cryptocurrency Regulations by Country*, Thomson Reuters (2022), https://www.thomsonreuters.com/en-us/posts/wp-content/uploads/sites/20/2022/04/Cryptos-Report-Compendium-2022.pdf.

[21] CoinMarketCap, *Today's Cryptocurrency Prices by Market Cap* (Sep. 7, 2022), https://web.archive.org/web/20220907050505/https://coinmarketcap.com/.

estimated range of crypto-assets trading on large platforms is over twice the amount of publicly traded stocks in U.S. markets.[22]

As crypto-asset platforms and services have become more commonplace, the risks may have become more salient among consumers, and the CFPB has noted a sharp increase in the number of complaints received related to these assets.[23] Consumers typically submit complaints about crypto-assets in the *virtual currency* product category, which has been an available on the CFPB's complaint form since August 2014.[24] Over the past two years, complaint volumes for total virtual currency complaints have increased from their levels in 2019 with sharp upticks in 2021 (Figure 1).[25]

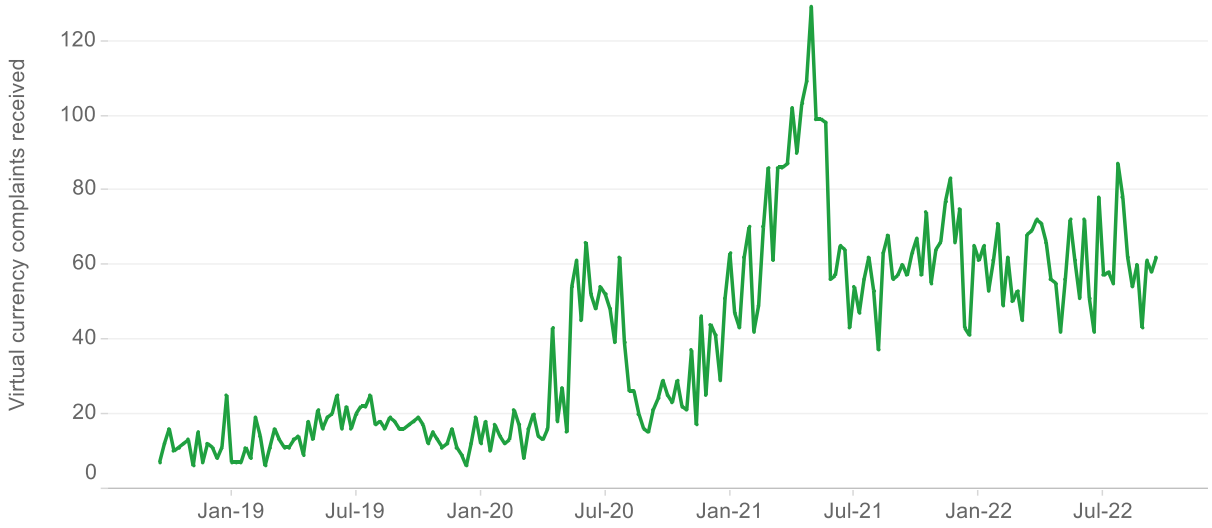
[22] Securities and Exchange Comm'n Chair Gary Gensler, *Testimony at Hearing before the Subcommittee on Financial Services and General Government U.S. House Appropriations Committee* (May. 17, 2022), https://www.sec.gov/news/testimony/gensler-testimony-fsgg-subcommittee. ("We review the disclosures and financial statements of more than 8,200 reporting companies.")

[23] *See* Consumer Fin. Prot. Bureau, Consumer Response Annual Report (Mar. 2022) at Section 4.6, https://files.consumerfinance.gov/f/documents/cfpb_2021-consumer-response-annual-report_2022-03.pdf.

[24] The list of product and service categories and subcategories on the CFPB's complaint form are intended to enhance usability for the consumer, rather than to reflect a legal determination by the CFPB. *See* Consumer Fin. Prot. Bureau, Note on user experience, https://portal.consumerfinance.gov/consumer/s/login/. Moreover, consumers who submit complaints related to crypto-assets may not know or self-report the details needed to determine which categories of consumer financial products or services may be implicated by the experiences described in their complaints.

[25] *See* discussion *infra* Section 2.

FIGURE 1: WEEKLY COUNT OF VIRTUAL CURRENCY COMPLAINTS, OCT. 2018 TO SEPT. 2022

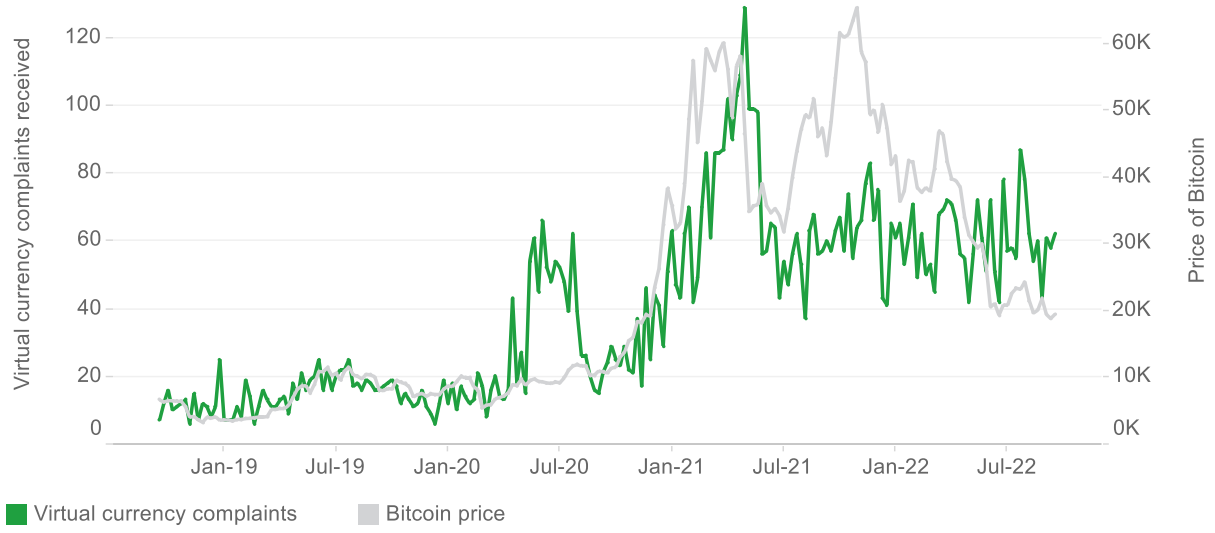


In addition, analyses suggest that complaints about virtual currency may increase when the price of Bitcoin (and crypto-assets generally[26]) increases (Figure 2).[27]

[26] Crypto-assets overall, and Ether in particular, appear to be highly correlated with Bitcoin. *See, e.g.,* Erik Norland *The Differences in Bitcoin and Ethereum Performance Drivers*, CME Group (June 9, 2022), https://www.cmegroup.com/openmarkets/economics/2021/the-differences-in-bitcoin-and-ethereum-performance-drivers.html.

[27] *See* Consumer Fin. Prot. Bureau, Digital Payments Conversation (Apr. 2022), https://files.consumerfinance.gov/f/documents/cfpb_digital-payments-conversation_slides_2022-04.pdf.

FIGURE 2: WEEKLY COUNT OF VIRTUAL CURRENCY COMPLAINTS AND BITCOIN PRICE, OCT. 2018 TO SEPT. 2022



Increasingly crypto-assets are being offered to consumers, including through consumer products such as credit, debit, and prepaid cards that offer rewards in crypto-assets and through crypto-asset products offered by person-to-person (P2P) payment platforms. Even large financial firms now offer and market crypto-asset custodial services to certain customers.

Given the growth in complaints related to crypto-assets, the CFPB is publishing this complaint report to share preliminary findings about the types of issues consumers face when using crypto-assets and the platforms in which they are stored, bought, sold, sent, received, loaned, and borrowed. This report describes complaints submitted to the CFPB about crypto-assets (Section 2), the issues consumers raise in their complaints (Section 3), and how these issues affect and pose specific risks to older consumers and servicemembers (Section 4). This report also discusses how the complaints the Bureau receives reflect on the marketplace (Section 5) and outlines some common risks consumers should consider when using crypto-assets and associated platforms (Section 6).

2. Complaint data

This report analyzes complaints submitted to the CFPB from October 2018 to September 2022.[28] When consumers submit complaints, the CFPB asks them to identify the consumer financial product or service with which they have a problem, the issue that best describes the problem, and the company to which they want to direct their complaint.[29] The CFPB then routes consumers' complaints directly to financial companies and works to get consumers a timely response. When the CFPB cannot send the complaint to a company, it refers the complaint to other federal agencies, such as the Federal Trade Commission (FTC).

The CFPB also makes a subset of this data publicly available in the Consumer Complaint Database (Database).[30] Complaints sent to companies for response are eligible to be published in the Database and are only published after 15 days or after the company responds, confirming a commercial relationship, whichever comes first.

There are two considerations researchers should keep in mind when analyzing complaints about crypto-assets:

1. When submitting complaints, consumers select the product or service that best describes the one that is the subject of their complaint.[31] Consumers generally select one of two categories when submitting complaints about crypto-assets: *virtual currency* and *mobile or digital wallet*. Consumers also submit complaints in other

[28] Complaint data in this report are current as of October 1, 2022. This report excludes some complaints that the Bureau received, including multiple complaints submitted by a given consumer on the same issue (i.e., duplicates), whistleblower tips, and complaints in which the CFPB discontinued processing because it had reason to believe that a submitter did not disclose their involvement in the complaint process. Complaint numbers are rounded throughout the report; therefore, numbers and percentages may not sum to 100%.

[29] *See generally,* Consumer Fin. Prot. Bureau, *Learn how the complaint process works*, https://www.consumerfinance.gov/complaint/process/. *See also* Consumer Fin. Prot. Bureau, *supra* note 23 at Section 1.

[30] *See* Consumer Fin. Prot. Bureau, Consumer Complaint Database, https://www.consumerfinance.gov/data-research/consumer-complaints/. *See also* Disclosure of Consumer Complaint Narrative Data, 80 FR 15572 (Mar. 24, 2015), https://www.federalregister.gov/documents/2015/03/24/2015-06722/disclosure-of-consumer-complaintnarrative-data.

[31] *See* Consumer Fin. Prot. Bureau, Consumer Complaint Form Product and Issue Options (Apr. 24, 2017), https://files.consumerfinance.gov/f/documents/201704_cfpb_Consumer_Complaint_Form_Product_and_Issue_Options.pdf (listing the current product and issue options available for consumers to select).

categories where crypto-assets have converged with more traditional banking products, such as credit cards offered by crypto-asset platforms.

2. Many virtual currency complaints are not published in the Database because they could not be sent to a company for response and thus do not meet the CFPB's publication criteria.[32] Instead, these complaints are referred to other regulatory agencies for handling, where appropriate. Last year, for example, about one quarter of virtual currency complaints were referred to other regulatory agencies. No matter if a complaint receives a company response, the CFPB shares complaint data with the FTC for inclusion in its Sentinel Network database and makes them available to federal and state agencies via the CFPB's secure Government Portal.[33] These complaints are also available to CFPB staff for review and analysis.[34]

2.1 Virtual currency complaints

From October 2018 to September 2022, the CFPB received more than 8,300 virtual currency complaints—the majority in the last two years. Consumers from all 50 states and the District of Columbia submitted complaints to the CFPB about virtual currency with the greatest number of complaints coming from California (Figure 3). In these complaints, the most common consumer-selected issue was fraud and scams, followed by transaction issues (Figure 4). Within the "Fraud or scam" complaints, consumers often report fraudulent transactions, theft, account hacks, and scams (Section 3).

[32] *See* Disclosure of Consumer Complaint Narrative Data, 80 FR 15572 (Mar. 24, 2015), https://www.federalregister.gov/documents/2015/03/24/2015-06722/disclosure-of-consumer-complaintnarrative-data.

[33] 12 U.S.C. 5493(b)(3)(D).

[34] *See* Consumer Fin. Prot. Bureau, *supra* note 23 at Section 1 (How the CFPB uses complaint information).

FIGURE 3: VIRTUAL CURRENCY COMPLAINT SUBMISSIONS BY STATE, OCT. 2018 TO SEP. 2022

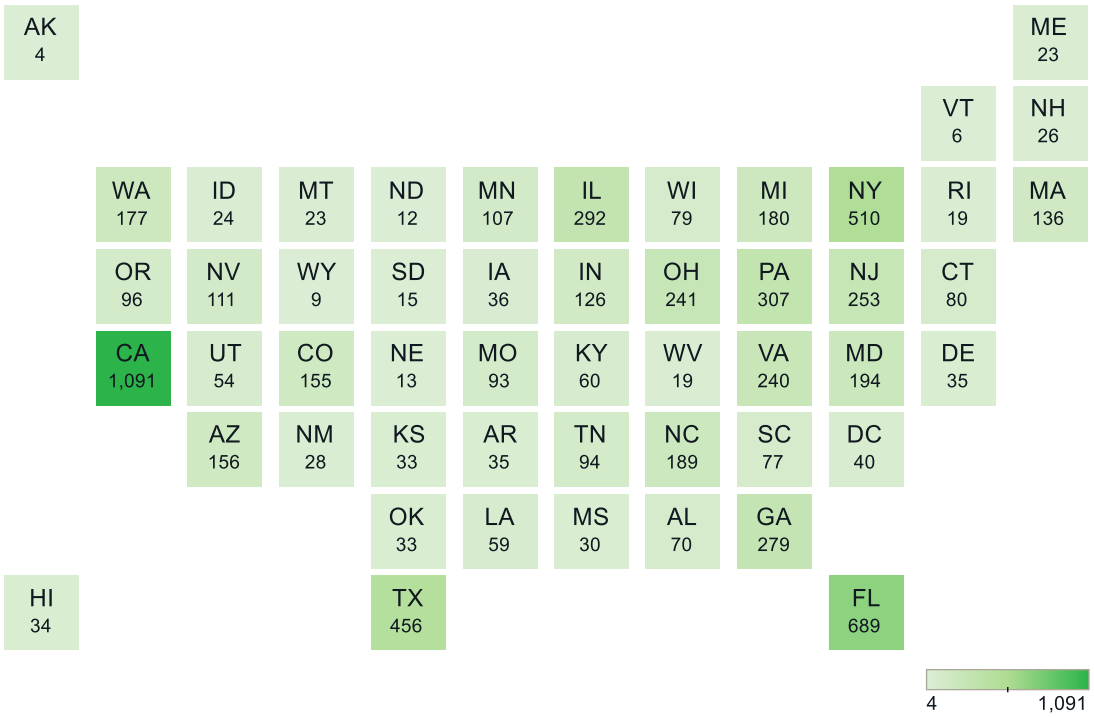
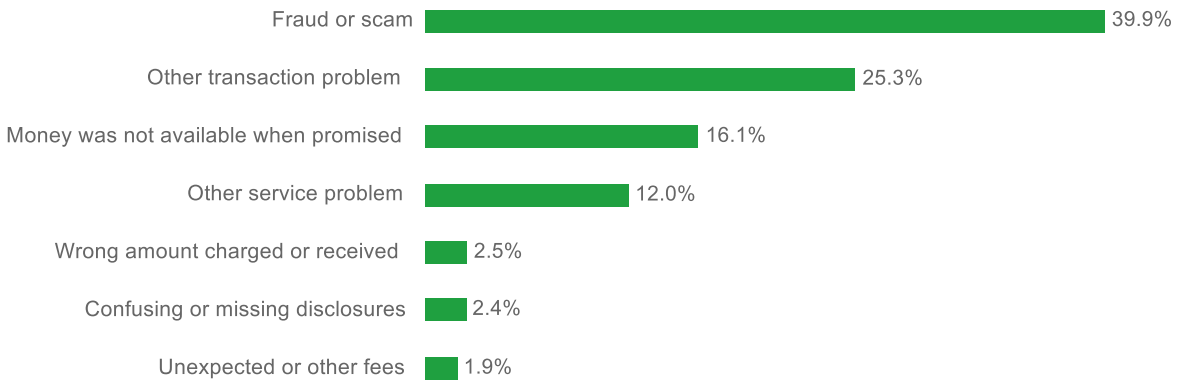
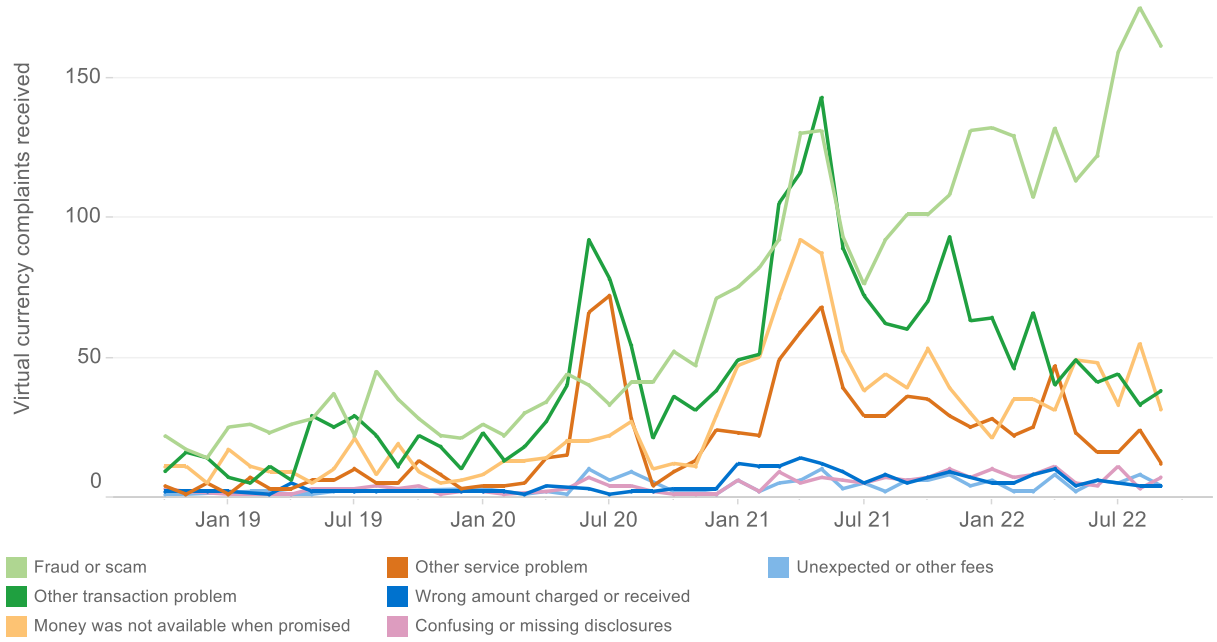


FIGURE 4: VIRTUAL CURRENCY COMPLAINTS BY ISSUE, OCT. 2018 TO SEP. 2022



Complaint volume related to fraud and scams has been increasing over time (Figure 5).

FIGURE 5: VIRTUAL CURRENCY COMPLAINTS BY ISSUE BY MONTH, OCT. 2018 TO SEP. 2022



Indeed, complaints about fraud and scams make up more than half of virtual currency complaints received thus far in 2022 (Figures 6 and 7).

FIGURE 6: VIRTUAL CURRENCY COMPLAINTS BY ISSUE, OCT. 2018 TO SEP. 2022

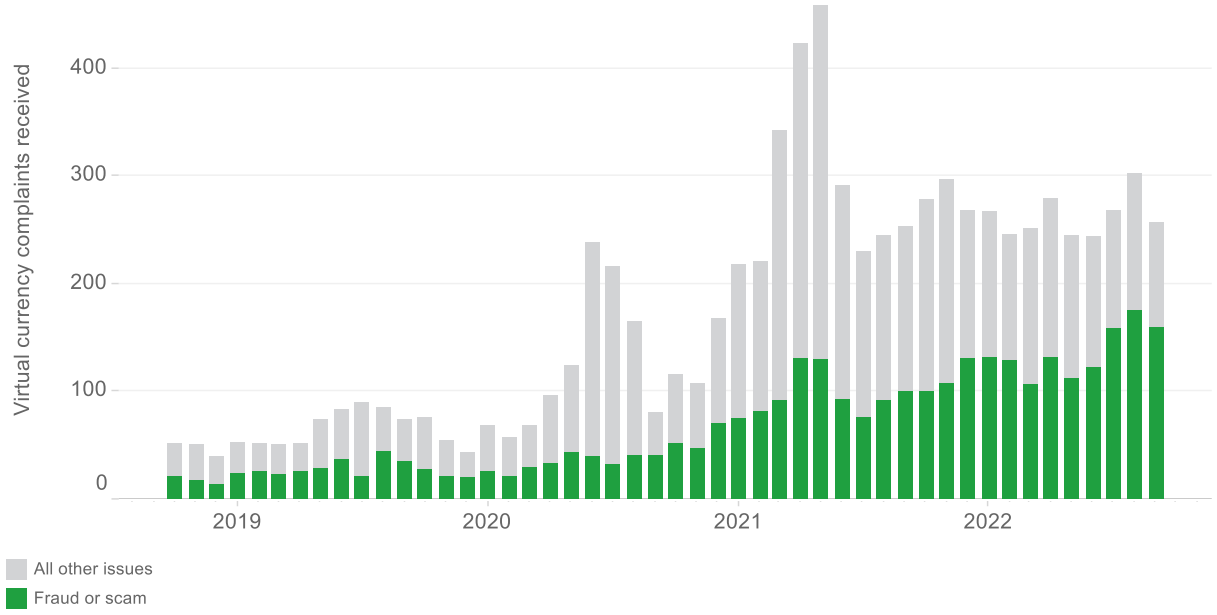
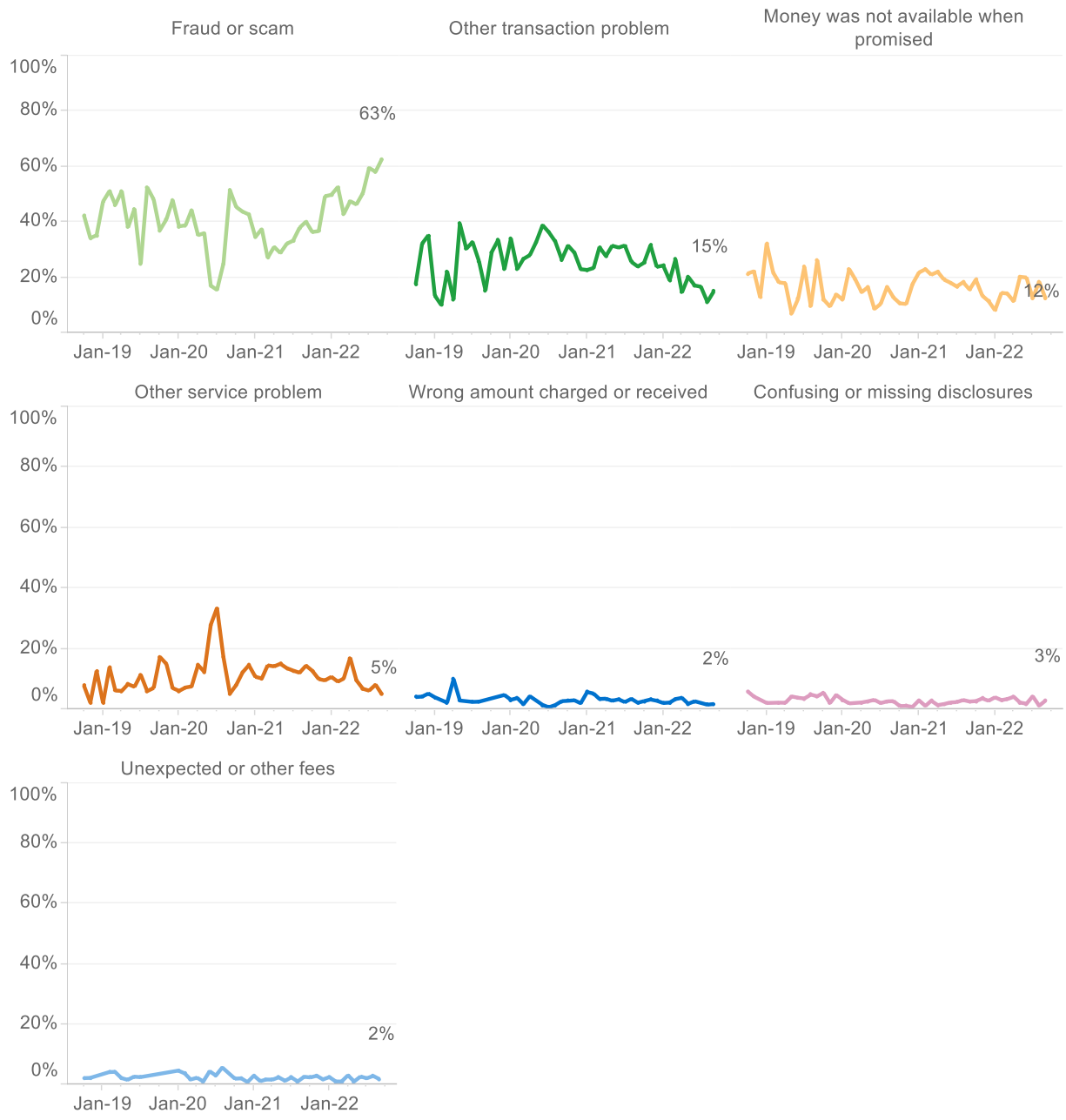


FIGURE 7: PERCENTAGE OF MONTHLY COMPLAINT VOLUME BY ISSUE, OCT. 2018 TO SEP. 2022



3. Consumer issues

Several broad issues predominate in CFPB complaints related to crypto-assets. First, consumers often report being victimized by frauds, theft, hacks, and scams.[35] Second, many users of crypto-asset platforms and wallets complain about issues resulting from the timing of transactions such as trades, the ability to execute transactions, and the ability to transfer assets between platforms. Third, many complaints are submitted by consumers who have trouble accessing accounts or assets held within accounts because of identity verification issues, security holds, or because of technical issues with platforms. Additionally, consumers having trouble getting help from a company's customer service is a common theme running through these issues.

Taken together, issues commonly identified in these complaints strongly suggest that consumers are at risk when seeking to acquire or transact with crypto-assets.

Complaints suggest that consumers that use or hold crypto-assets need to be aware of two distinct kinds of risk. First, crypto-assets are subject to the expected financial risk of loss associated with speculative assets. Second, crypto-assets are vulnerable to risks of cyber and data security vulnerabilities, transaction processing issues, technical platform issues, and other kinds of non-financial loss. In addition, these distinct risks have spillover effects; for example, discovery and exploitation of cyber and data security risks in a crypto-asset can result in price changes as market sentiment adjusts to these risks. Technical problems at platforms can also impact asset prices.

3.1 Fraud, theft, hacks, and scams

Complaints suggest that crypto-asset platforms and wallets are often a direct target of fraud and theft. For example, some technically sophisticated thefts have been perpetrated by intercepting

[35] Throughout this report, the CFPB highlights consumer narratives. The CFPB is sharing these narratives to better illustrate how consumers currently describe this market and the issues they experience. Inclusion of narratives in this report are for illustrative purposes only and do not represent a determination made by the CFPB about its legal authorities. *See also* discussion *supra* note 24.

SMS messages using a so-called "SIM-swap" to exploit two-factor authentication at crypto-asset platforms. For example, one consumer stated:

> I got SIM hacked on [date], i.e., Hackers took over my phone temporarily via SIM transfer and my Gmail permanently. After I got my phone number back from [cell phone provider] I instantly tried locking my account on [crypto-asset platform]. When I couldn't get in, I finally found a phone number where you can do that, even though it's just a bot. I also wrote an email to [crypto-asset platform] support and they only responded with a generic email about security and mentioned reinstalling the account via email (which just had been hacked and is still compromised!?!).
>
> I have not received any updates if the hackers were successful in transferring any crypto out (I'm afraid so) or if they are locked out or what the actual damage is, etc. And I read in many forums like [social media site] that [crypto-asset platform] often takes their sweet time to respond, up to weeks and months! How is that possible for such a big company with a huge IPO to ignore their customer safety this badly? This contributes to the bad image crypto has as enabling criminals…[36]

In its response, the company stated that those transactions were irreversible.

Other fraudulent behavior aimed at crypto-assets involves phishing, social engineering, or both to gain access to personal and account information. This personal information is then used to gain access to a consumer's crypto wallet and crypto-assets. As was the case in the above example, companies often responded to these complaints by telling consumers that these transfers are not reversible because of the nature of the crypto-asset that was stolen, and by noting that consumers are responsible for the security of their accounts. Some consumers stated that they have lost hundreds of thousands of dollars due to unauthorized account access.

For example, one consumer shared:

> [On date] I clicked a phishing link saying my [crypto-asset platform] account was compromised. I reset my password on the internet browser link and then logged in on the app where I saw different tokens being converted into [crypto-asset]. I called [crypto-asset platform] to freeze my account and did it virtually as there are no live people. I got an email saying my funds were frozen. Then I got an email saying all of my funds were transferred out into a different wallet. I did not do any

[36] Consumer Complaint 4356993, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4356993.

> two-factor authentication as I am supposed to. I did not authorize any funds transferring out. I also did not authorize any computer besides my phone to complete any transaction ever. Someone took around 10,000 from me, which [crypto-asset platform] shouldn't have allowed within seconds of a password being changed. They also could have reversed or stopped this as I was on the phone within seconds of changing my password. I have contacted them repeatedly, but it has been over two weeks now without any personalized response or acknowledgement. They said they transferred my case to a specialist and are not responding to any more emails.[37]

In its response, the company stated it was unable to reverse the transaction. Indeed, many crypto-asset firms reference the immutability of many blockchain transactions to tell consumers there is no way for fraudulent transactions to be reversed or, in some cases, for the consumer to be compensated.

Scams that use crypto-assets as a premise are also common. In many of these complaints, consumers are victimized by individuals that frequently offer promises of large returns that never materialize. Often these scams involve advertising, outreach, or other marketing on social media platforms like Facebook, Instagram, and YouTube. Some consumers claimed that advertisements on these platforms directly promoted scams.[38]

In one complaint, a consumer reported one such scam:

> [H]ere was a YouTube video saying free [crypto-asset] if you send it to a certain wallet address: [URL]…
>
> Amount: [about 4,000] [crypto-asset] ([about 5,000] USD)…
>
> I sent the [crypto-asset] not knowing it was a scam. I would like my money back. I saved it for years and was investing it. I didn't know this was a scam.[39]

In its response, the company stated that it would be impossible to recover the lost assets.

---

[37] Consumer Complaint, 4317161, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4317161.

[38] Tech Transparency Project, Google Helps Scammers Target Americans Seeking Student Loan Relief (July 13, 2022), https://www.techtransparencyproject.org/articles/google-helps-scammers-target-americans-seeking-student-loan-relief.

[39] Consumer Complaint 4323561, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4323561.

According to the FTC, the most common type of crypto-asset scams is "investment scams," similar to the example above.[40] Another common type of scam involves a person or entity impersonating a business or government.

In other complaints, crypto-assets were targeted in romance scams or merchant scams. Like prepaid cards and cash, the ability to obscure the transfer of assets[41] makes crypto-assets a useful target for scammers in many cases.[42] In fact, many hackers looking to exploit vulnerable technical systems have recently shifted their focus to crypto-asset markets.[43]

According to the FTC, romance scams—where scammers play on a victim's emotions to extract money—are also increasingly common.[44] Some of these scammers combine romance scams with a technique law enforcement refers to as "pig butchering," where fraudsters pose as financial successes and spend time gaining the victim's confidence and trust, coaching victims through setting up crypto-asset accounts.[45] Data from the CFPB shows that romance scams are particularly common among older consumers.[46] One older consumer told the CFPB:

> I connected with someone on [social media] who had a profile as an instructor at the [a military school] in [location] and who later went on to say that he was being sent overseas again by the CIA on an undercover assignment for our country. He also said he had made me his sole contact and that his "handler" would text me information to send to him once he was in Kazakhstan so that he could access the

[40] Fed. Trade Comm'n, *supra* note 1.

[41] There are a number of techniques for obscuring crypto-asset transfers, including chain hopping, utilizing opaque "Layer 2" protocols, the use of mixers and tumblers, and converting one crypto-asset to an anonymity-enhanced crypto-asset, also known as "privacy coins." *See* FSOC Report on Digital Assets, *supra* note 6 at 68.

[42] Relatedly some median reports suggest that the availability of crypto-assets has enabled more sophisticated ransomware attacks on business. *See* Greg Myre, How Bitcoin Has Fueled Ransomware Attacks (June 10, 2021), https://www.npr.org/2021/06/10/1004874311/how-bitcoin-has-fueled-ransomware-attacks.

[43] *See, e.g.,* Ruholamin Haqshanas, *Hackers Stole USD 670M from DeFi Projects in Q2, Up by 50% from Q2 2021*, Crypto News (July 6, 2022), https://cryptonews.com/news/hackers-stole-usd-670m-from-defi-projects-in-q2-up-by-50-from-q-2021.htm ("Hackers and fraudsters stole a total of USD 670.7m from various crypto protocols during the second quarter of the year, according to a report by major bug bounty and security services platform Immunefi … The report claimed that the bulk majority of the losses (almost 97%) happened as a result of hacks. It added that blackhat hackers are now primarily targeting and exploiting DeFi projects, as 49 out of 50 instances involved DeFi protocols … Glassnode also noted that hackers have recently shifted their focus from crypto exchanges and centralized crypto platforms toward DeFi projects mainly because they are open-source, meaning their code is publicly visible.").

[44] Emily Fletcher, *Data Spotlight: Reports of romance scams hit record highs in 2021*, Federal Trade Comm'n (Feb. 10, 2022), https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/02/reports-romance-scams-hit-record-highs-2021.

[45] *See* FBI Miami Field Office and the Internet Crime Complaint Center (IC3), *Cryptocurrency Investment Schemes* (Oct. 3, 2022), https://www.ic3.gov/Media/Y2022/PSA221003.

[46] Consumer Fin. Prot. Bureau, *supra* note 27.

> ASA/FMC account and send money through to my credit cards so I could take out cash advances and send them to him via bitcoins for him to conduct the project he was sent on assignment to do. Money started showing up in some of my credit card accounts and I was eventually sent a "promissory agreement" on what appeared to be real CIA letterhead, so I went forward sending bitcoins to him thinking I was helping not only him but our country. Eventually it became clear that it was a scam after all of the money sent through to my credit card accounts was sucked back out after I sent him the funds…I am stuck with approximately $100,000 in debt…[47]

In its response, the company said it was unable to help the consumer recover the lost assets. Section 4.1 discusses issues facing older consumers further.

3.2 Transactions issues

Another common set of issues identified in complaints involve transaction issues when buying and selling crypto-assets, or when attempting to withdraw assets or U.S. dollars from crypto platforms. Consumer complaints suggest that many consumers have trouble executing transactions, especially during times of increasing crypto-asset prices (Section 1, Figure 2). These consumers often complain that they cannot complete transactions promptly, resulting in losses or the inability to realize profits. As one consumer stated:

> [On date] [crypto-asset platform] app shut down around 10am with all my cash and cryptocurrency in it. Has been having 'technical difficulties' for the past 6 hours, causing me to be unable to buy/sell cryptocurrency. As a result, I have not been able even see my account and have lost a lot of money since I am not able to access or trade during a downturn in the cryptocurrency market.[48]

In its response to the consumer, the company cited its terms and conditions, which state in part "that you acknowledge and agree that we will not be liable, and you will not hold or seek to hold us liable for any technical problems, system failures and malfunctions, communication line failures, equipment or software failures or malfunctions, system access issues, system capacity issues, high internet traffic demand, security breaches and unauthorized access, and other similar computer problems and defects."

---

[47] Consumer Complaint 4255326, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4255326.

[48] Consumer Complaint 4160391, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4160391.

Other consumers had issues with compatibility between crypto-assets they owned, and those that could be used on a specific crypto-asset platform. For example, some consumers stated that they could not sell assets after learning that they would be de-listed by a platform (so that the consumer is no longer able to transact in that particular asset). Other consumers experienced losses when attempting to transfer incompatible assets between different wallets or crypto-asset platforms. Because several major crypto-assets have been "forked," or split off into separate blockchains, consumers are often unaware of the incompatibility between their assets until attempting to make a transfer. In these situations, consumers complain about difficulty recovering their transferred assets. As one consumer stated:

> Hello, I have problem with [crypto-asset platform] company about a crypto transaction. I tried to contact the company, but they don't answer my email and they don't have a number to call. On the [date] in my [crypto-asset platform] wallet I sent some 20,000 [crypto-asset] from [crypto-asset platform] wallet to my [crypto-asset] Wallet in [URL]. the transaction was approved but the funds never arrived. They told me that I can't send swap different currency. So, I gently asked them to reverse the transaction, but they told [me] that they can't, and my money are lost. The value of these funds now is [over $15,000].[49]

In its response, the company stated that the consumer had been given warning messages not to attempt the transfer, and that it was unable to help recover the assets.

3.2.1 Undisclosed or unexpected costs

Some consumers complained about undisclosed or unexpected costs on crypto-asset platforms, or claims there were no fees when, in reality, the consumer noticed a large cost in the form of a large spread.[50] One consumer mentioned misleading terms indicating that converting from one crypto to another would be "free":

> [Under] the guise of "Free" conversion from crypto to crypto [crypto-asset platform] charges a huge spread when making these "Free" [conversions]. They need to disclose the spread and the cost of that crypto to crypto transfer.[51]

---

[49] Consumer Complaint 4203691, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4203691.

[50] The spread refers to the difference between two prices, commonly, the gap between the price an asset can be purchased at (the bid) and the price an asset can be sold at (the ask).

[51] Consumer Complaint 5154181, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5154181.

Another consumer complained about discrepancies between listed prices and the amounts they received when selling an asset or the high fees for completing transactions:

> On [date], I executed a trade of [crypto tokens] using the [crypto-asset platform] App. At this time the spot price on [the platform] was ~.46-.47 USD. As communicated through the [platform's] App, when I agreed to sell my tokens, my portfolio was valued at ~42,XXX.XX USD. As the transaction was completed moments later, my portfolio, then in USD, was valued at [under $32,000] - an evaporation of ~11,XXX USD… I fully understand slippage is to be expected while trading crypto-assets, especially on [the app], however a delta of north of 20% is not slippage but an error (at best) and one that hopefully is corrected swiftly.[52]

In its response, the company stated that this resulted from the difference between the "spot" price and the price locked in when the trade is executed, and that the amount the consumer received from the sale was accurate.

Another consumer described extremely large spreads and price discrepancies:

> On 10/29/2021, I had total 61259495 [crypto-asset] coins in my account. When I looked at the home screen on [crypto-asset platform] it was showing current value 4879.85$ and checked [crypto-asset] current market price 0.00007827$.
>
> Then I tried to sell some coins so went into trade -> selected [crypto-asset] and selected max (coins) for sale and went on confirm screen and it was showing sale price 0.00007127$ and total value 4366.01$…
>
> For next 2 weeks, I tried same thing for about 7-8 times and noticed that when I try to see coins it is showing higher price when I initiate the sale and it suddenly changes at the final confirmation page. It is almost 20% less…This seems like a software trick to make money and scam people.
>
> I raised this issue multiple times with [crypto-asset platform] but have not received satisfactory response.[53]

[52] Consumer Complaint 4345742, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4345742.

[53] Consumer Complaint 5510377, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5510377.

In its response, the company stated that "a price increase or decrease from the reference price to the execution price could be due to volatility in the value of the digital asset being bought or sold."

Finally, another consumer complained that a crypto-asset platform would not let them close an account until their balance was zero, but the fee to withdraw the remaining U.S. dollars exceeded the amount in the account, so the consumer could not close their account. The consumer describes also being unable to sell their crypto-assets due to needing to verify their account through a wire transfer, which also incurred a fee:

> Created an account...and deposited $100, bought 18+ [crypto-asset] coin and have approximately $9 dollars in [crypto-asset]. Want to close account and they require zero balance, but I can't sell anything because they want a wire transfer from my bank (deposit more money) which costs $25 both ways which is crazy and unfair since they let me in without a wire transfer.[54]

In its response, the company stated it had requested a wire transfer to verify the bank account was controlled by the consumer. After a discussion with the consumer, the company refunded the consumer's initial debit card deposit and closed the account.

3.2.2 Account access and verification

Consumers also often complained about account issues related to verifying their identity or confirming account ownership, which led to them being locked out of their accounts. Some consumers pointed to specific large transactions that resulted in these issues. Others claimed that they were asked for additional identity verification documents after using a platform for some time. Consumers reported multiple attempts to resolve issues by uploading documents, such as a driver's license. These customers often complained about poor or non-existent customer service. Some consumers claimed that accounts remained frozen for weeks or months. For example, according to a consumer:

> I was asked to verify again in December and provided them with a passport photo which was accepted and got the account unrestricted but then a few months later I received an email telling me my account would be restricted again as my account was under review, a process that they said would take a few days. I don't mind having my buy and sell capabilities suspended but I can't even send my assets to a different exchange. They ignore my emails, customer support requests and tweets

[54] Consumer Complaint 5047875, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5047875.

> and it seems like my money is gone forever, they have taken it with no route to get it back. [The crypto-asset platform] are doing this to many people and it's unacceptable…I just want some clarity, why is my account under review? Is there any document I can provide to resolve this issue? In an ideal world I would like my account back, able to buy, sell and send my cryptocurrency but at this point I have lost all trust in [the crypto-asset platform] so I would just like to move my funds to a better exchange that have never treated me like this.[55]

In its response, the company apologized for the experience, reported that the issue had been resolved, and offered about twenty dollars as a gesture of apology.

3.3 Customer service issues

Poor customer service is a common theme across complaints.[56] It is also a recurring issue in complaints about crypto-assets generally. Consumers sometimes complained about the difficulties they face in getting in touch with customer service representatives at crypto-asset platforms and getting the help they need. For example, one consumer complained:

> I'd like to submit a formal complaint about [a crypto-asset platform], their customer service and the quality of their service in general.
>
> Ever since I created an account with [a crypto-asset platform] approximately six months ago, I have encountered number of issues. Even though I went through all the required steps of verification, I would experience the issues with [the crypto-asset platform's] system that would not allow me to purchase cryptocurrency, or sell cryptocurrency, or transfer the money from my checking account to USD wallet on [the crypto-asset platform] or it would not allow me to plug in my debit card.
>
> When I would write a message to customer service, it would take them days to respond. It would be weeks before they do anything. And they would ask me to email them very sensitive personal financial information even though I already submitted that information before, even though everything was verified by their system, even though I have already made purchases and money transfers before. But they would be asking to email them more information like banking statements for the last few months etc. And then they would say that they had to do that to

[55] Consumer Complaint 4137827, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4137827.

[56] *See generally* Consumer Fin. Prot. Bureau, *supra* note 23.

> white-list my account. I don't even know what that means. When I would ask them questions why my account still didn't work even though I went through all the proper notification steps, and why they are requesting more of the sensitive documents, they would not answer questions, and they would be kind of rude in their email response.[57]

In its response, the company stated it would try to be more responsive in the future.

Some consumers reported being unable to get their problem resolved because they cannot reach a human at the company. For example, one consumer stated:

> My family and I have 4 accounts with [crypto-asset platform]. All of a sudden, we are still able to log into our accounts, but the accounts are "restricted" and it is NOT possible to make any transactions or close the account. There is NO one at the company to talk to…only website inquiries. There are NO options to choose from regarding a "restricted account." I have used other forms on their website to submit an inquiry but for the last 4 weeks NO one has responded. I need someone at your office to either, (1) contact [crypto-asset platform] for me, (2) email the a [sic] phone number at [crypto-asset platform] where I can actually speak to someone.[58]

Because of the price volatility of the underlying crypto-assets, consumers often pointed out that failure to provide timely customer service exposed them to unnecessary risks. One consumer stated:

> I have an account with [crypto-asset platform] (for 3 years) where I buy and trade [crypto-asset] as an investment opportunity. I have funds locked in a [crypto-asset] Vault that need to be moved to my [crypto-asset] wallet (part of their normal security process). There are multiple layers of security, and 2 email addresses are required. One of my old email addresses is no longer active so this is preventing me from receiving an authentication email to get my funds. [The crypto-asset platform] no longer has a phone line for customer service (I assume due to covid) so email is the only customer service available. I first emailed them about this problem Dec.3, receiving a generic email thanking me for contacting them and someone would be in touch soon. I waited one week, heard nothing, email—same generic response back. Emailed again every day from the 11-18. Finally on Dec 19th

[57] Consumer Complaint 3992322, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/3992322.

[58] Consumer Complaint 4133656, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4133656.

> I get a response saying the only way to fix this is to have them move the funds to my wallet, delete the vault, and then I could create a new vault and be back in shape. They sent a link asking me to verify my ID … which I did. On the 21st I get the same email asking me to verify again which I did and got confirmation that it was verified. Today (12/28) they email me saying if they don't hear from me my case will be closed due to no action on my part. BEYOND FRUSTRATING that my investment money is locked with no access and their lack of customer service is causing me to lose money every day as the [crypto-asset] market fluctuates like a stock price…[59]

In its response, the company apologized for the experience, reported that the issue had been resolved, and offered ten dollars as a gesture of apology.

3.3.1 Scammers impersonating customer service representatives

Lack of customer service options for many crypto-asset platforms and wallets creates opportunities for social media scams where attackers pretend to be customer service representatives to gain access to customers' wallets and steal crypto-assets.[60] For example, on certain social media sites, merely mentioning certain crypto-asset wallet names in a post often leads to many bot-type accounts responding with (false) offers to help.[61] In actuality, these are attempts to scam a user out of their crypto-assets. The lack of dedicated support for one wallet provider may be contributing to a plethora of scams, enough that the provider itself posted tips on avoiding these scams on social media,[62] and the parent company of the provider wrote an entire blog post devoted to explaining how to avoid these scams.[63] Impersonation of customer service representatives are not limited to companies with no customer service divisions;

---

[59] Consumer Complaint 4033764, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4033764.

[60] See Will Gendron, *Scammers are impersonating MetaMask tech support on Twitter*, Input Mag (Jan. 21, 2022), https://www.inputmag.com/tech/beware-of-scammers-impersonating-metamask-support-on-twitter.

[61] Lawrence Abrams, *Twitter bots pose as support staff to steal your cryptocurrency*, Bleeping Computer (Dec. 7, 2021), https://www.bleepingcomputer.com/news/security/twitter-bots-pose-as-support-staff-to-steal-your-cryptocurrency/.

[62] @MetaMask, Twitter (May. 2, 2022, 9:33 PM), https://twitter.com/MetaMask/status/1389030423611658241 ("An easy easy way to avoid this kind of phishing attack is to ONLY seek support from WITHIN the app you want help on!").

[63] Joel Willmore, *Spoofing, Sweepers, and Clipboard Hacks: How To Stay Safe From Scams*, Consensys (Jan. 13, 2022), https://consensys.net/blog/metamask/spoofing-sweepers-and-clipboard-hacks-how-to-stay-safe-from-scams/.

scammers impersonate customer service representatives even from companies that have such a division.

For example, in a complaint to the Bureau, a consumer reported being at risk of losing nearly $40,000 when they were contacted by a scammer who claimed to be an employee of a crypto-asset platform who needed to help them unlock their account.[64]

In another complaint, one consumer complained about losing tens of thousands of dollars to someone that the crypto-asset platform later determined was a scammer impersonating a customer service representative for that platform:

> I'm filing a complaint against [a crypto-asset platform]. $20,000+ of my digital assets were stolen from the [the platform]. [The platform] is not taking responsibility for the gross negligence on their part. My account was initially hacked in August 2021 and I immediately informed them about it. They failed to protect my account and did not respond to my concerns until nothing was left in my portfolio… zero, zilch, nada! I could not even access my account to withdraw the remaining funds. [The platform] kept reiterating that transactions on the blockchain are irreversible. But I informed them of the initial incident when I still had around 90% of my funds left. If transactions are irreversible, they should have protected or froze my account after I first found out it was hacked. I asked [the platform] to secure my account before the hacker took out the remaining funds in my account. They did not protect my account. They ignored my emails. When they finally responded, I was left with ZERO balance in my account…[65]

In its response, the company agreed to reimburse the consumer for their lost funds.

3.3.2 Scammers impersonating influencers on social media

Some scammers try to use social media posts by crypto-asset influencers and celebrities to trick victims. For example, a scammer may impersonate a celebrity, influencer, or prominent crypto-asset developer or development team using verified (sometimes stolen) social media accounts or promotional videos to promote giveaways or "double your crypto" scams.[66]

---

[64] Consumer Complaint 4716709, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4716709.

[65] Consumer Complaint 5191424, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5191424.

[66] Molly White, *'Double your money' scammers capitalize on Ethereum merge*, Web3 is Going Great (Sep. 14, 2022), https://web3isgoinggreat.com/single/double-your-money-scammers-capitalize-on-ethereum-merge.

A consumer complained about losing over ten thousand dollars' worth of crypto-assets to a scammer impersonating a crypto-asset development team:

> Commencing on or about November 15, 2021, I fell victim to a multilayered scam operation orchestrated by Fake Representatives of [crypto-asset] Giveaway (the "Scammer"), using web address (the "Scam Website"), all of which aim at contributing to the goal of robbing and defrauding clients, through a predetermined cycle of the client's losses to their gains. The equivalent of 10,177.70 USD (5000.18 [crypto-asset]) was transferred from my wallet utilizing [crypto-asset platform] services.[67]

The CFPB has also received complaints from consumers about scams being promoted by scammers impersonating crypto-asset developers and founders on other websites such as YouTube. Another form of this scam is impersonating the official accounts of governments or nation states. In March 2022, the FTC warned of scammers soliciting crypto-asset donations to allegedly help people in Ukraine; instead, donations go to the scammer's crypto-asset wallet.[68]

3.4 Frozen accounts and platform bankruptcies

Several large crypto-asset platforms have recently either frozen customers' account withdrawals, filed for bankruptcy protection, or both. These failures have impacted millions of consumers.[69] At least one of the firms repeatedly misrepresented through official channels the nature of its Federal Deposit Insurance Corporation (FDIC) insurance, leading to confusion among consumers and, ultimately, a cease-and-desist order by other agencies.[70] Other crypto-asset

[67] Consumer Complaint 5868008, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5868008.

[68] Rosario Méndez, *Donating with crypto? Watch out for scams*, Fed. Trade Comm'n (Mar. 25, 2022), https://consumer.ftc.gov/consumer-alerts/2022/03/donating-crypto-watch-out-scams.

[69] *See, e.g.,* Cision PR Newswire, *supra* note 8 ("Total funded accounts reached 1,190,000 as of March 31, 2022") *See also* Vicky Ge Huang, *supra* note 8; Vicky Ge Huang, *supra* note 8.

[70] *See, e.g.,* Fed. Deposit Ins. Corp., Joint Letter Regarding Potential Violations of Section 18(a)(4) of the Federal Deposit Insurance Act (July 28, 2022), https://www.fdic.gov/news/press-releases/2022/pr22056a.pdf. *See also* Press Release, Fed. Bd. of Governors of the Fed. Rsrv. Sys., FDIC and Federal Reserve Board issue letter demanding Voyager Digital cease and desist from making false or misleading representations of deposit insurance status (July 28, 2022), https://www.federalreserve.gov/newsevents/pressreleases/bcreg20220728a.htm.

websites and platforms have since received cease-and-desist orders from the FDIC regarding misleading language about FDIC insurance.[71]

The CFPB has received complaints from consumers related to their inability to access U.S. dollars in their account. A consumer's complaint highlighted that the company's actions contradict the disclosures it had made to consumers:

> I have an account with [crypto-asset platform]. They have recently froze my account and they are not allowing me any withdrawals at the moment. According to the disclosure these should not be affecting me. I have provided a copy of the disclosure to complete the research of this complaint.[72]

Another consumer complained about their inability to withdraw funds:

> I deposited $65k into [a digital] wallet and they just froze my account for withdrawing money. This is hard earned money I need to pay for medical expenses.[73]

Another consumer described how the company was unresponsive to their request for a wire transfer:

> I have around $150,000 worth of USD and digital currency there (mostly USD which they claim is FDIC insured…) - I want to withdraw all of my USD as quickly as possible because I am worried they will freeze withdrawals soon, the way the [another crypto-asset platform] did. I have been withdrawing $10,000 / day for 6 days now, but I decided early yesterday to open a support ticket requesting a wire transfer because their website says they offer wire transfers for $50 per. They have not responded to this ticket and a friend of mine opened a ticket days ago requesting the same thing and got no response.[74]

Still another consumer reported the same issue with a wire transfer:

> On [date and time] I provided instructions for an outgoing wire in the amount of [over $200,000]. I then emailed the company and have not received the wire nor

[71] Press Release, Fed. Deposit Ins. Corp., FDIC Issues Cease and Desist Letters to Five Companies For Making Crypto-Related False or Misleading Representations about Deposit Insurance (Aug. 19, 2022), https://www.fdic.gov/news/press-releases/2022/pr22060.html.

[72] Consumer Complaint (on file with author).

[73] Consumer Complaint (on file with author).

[74] Consumer Complaint (on file with author).

> response from the company since that time. The wire was coming to a personal bank account of mine. I also do know that they got my emails because they responded to other mails.[75]

The CFPB also received complaints about another crypto-asset platform that froze consumers' assets and recently filed for bankruptcy protection. For example, a consumer described how the company had misled them:

> I am a customer with [a crypto-asset platform] that recently froze withdrawals. I had no loan products and only bought a stablecoin, [crypto-asset], which is pegged to the US dollar and has not been depegged. [The crypto-asset platform] misled me when I deposited approximately $5000 USD into their exchange with the promise that it could be withdrawn at will. My most recent balance is approximately $5300 [crypto-asset].[76]

3.5 Crypto-asset card complaints

Many crypto-asset platforms offer products marketed by companies as credit, debit, or prepaid cards with various features, including offering rewards in crypto-assets. Consumers submitted complaints about credit cards and prepaid cards in which they reported several problems using these crypto-asset cards, including the inability to make purchases, issues closing their account, rejecting their claims for reimbursement on fraudulent charges, or failing to receive advertised rewards. A consumer stated that they would like "my credit card to work when I use it, or to know why a certain retailer or transaction was blocked," and was not receiving this resolution from their crypto-asset reward card:

> I have the [crypto-asset platform] card, it regularly gets rejected, or stops working for no reason. I have opened up multiple tickets, and there is never any resolution, they just say that 'a fraud prevention algorithm prevented the transaction'. And this is after multiple support calls, where they are completely unable to tell me why my card isn't working.[77]

---

[75] Consumer Complaint (on file with author).

[76] Consumer Complaint 5675592, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5675592.

[77] Consumer Complaint 5787938, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5787938.

A consumer complained about not receiving rewards from their credit card, and then having trouble closing their account once they were told they will not receive the advertised crypto-asset rewards feature:

> I obtained the [crypto-asset platform] card because they allowed your rewards to be used to buy Crypto … Now they say that they don't know why the feature is not working and there is nothing they can do about it. Now, I asked them to close the account and they are giving me the run around saying I need to contact a third-party bank?![78]

Another consumer complained that they failed to receive an advertised sign-up bonus after meeting the terms specified by the rewards card. The company replied that its offer may be redeemed only by the eligible participant and that "such eligibility to be determined by [company] in its sole discretion."[79]

[78] Consumer Complaint 5029504, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5029504.

[79] Consumer Complaint 5566854, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5566854.

4. Impact on special populations

The use of crypto-assets varies across different communities, and some reports have noted concerns about risks crypto-assets pose to younger populations[80] and Black and Latino communities.[81] Older consumers and servicemembers are just two populations of special interest to the CFPB, as they can be disproportionately impacted by problems with financial products and services and can also face special concerns and constraints on solving these problems.[82] For these populations, crypto-assets are no exception.

4.1 Older consumers

Cybercrime losses in general among older consumers are increasing steeply, in general. A 2021 report from the FBI states, "[i]n 2021, over 92,000 victims over the age of 60 reported losses of $1.7 billion to the [Internet Crime Complaint Center] IC3. This represents a 74 percent increase in losses over losses reported in 2020."[83] The CFPB has observed an increase in complaints about crypto-assets submitted by older consumers (Figure 8), especially complaints involving

[80] *See, e.g.*, Cheyenne DeVon, "Only about 30% of millennials are comfortable investing in crypto, down from about 50% in 2021: 'The shine has come off these coins'", CNBC (Sep. 29, 2022), https://www.cnbc.com/2022/09/29/millennial-investors-are-getting-less-comfortable-with-cryptocurrency.html.

[81] *See, e.g.*, Terri Bradford, *The Cryptic Nature of Black Consumer Cryptocurrency Ownership*, Federal Reserve Bank of Kansas City (Jun. 1, 2022), https://www.kansascityfed.org/research/payments-system-research-briefings/the-cryptic-nature-of-black-consumer-cryptocurrency-ownership; Paulina Cachero, *Crypto Collapse Threatens to Leave Black, Hispanic Investors Further Behind*, Bloomberg (Jul. 7, 2022), https://www.bloomberg.com/news/articles/2022-07-07/crypto-collapse-threatens-to-leave-black-hispanic-investors-further-behind.

[82] "Servicemembers" and "older consumers" are both self-identified. Servicemembers refers to servicemembers, veterans, and military families. "Older consumers" refers to consumers who voluntarily reported their age as 62 or older.

[83] Fed. Bureau of Investigation, Elder Fraud Report (2021), https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3ElderFraudReport.pdf.

frauds and scams (Figure 9). Other research also indicates that older consumers' losses as a result of crypto-asset scams are larger than any other age group.[84]

FIGURE 8: COUNT OF VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY OLDER CONSUMERS, OCT. 2018 TO SEPT. 2022

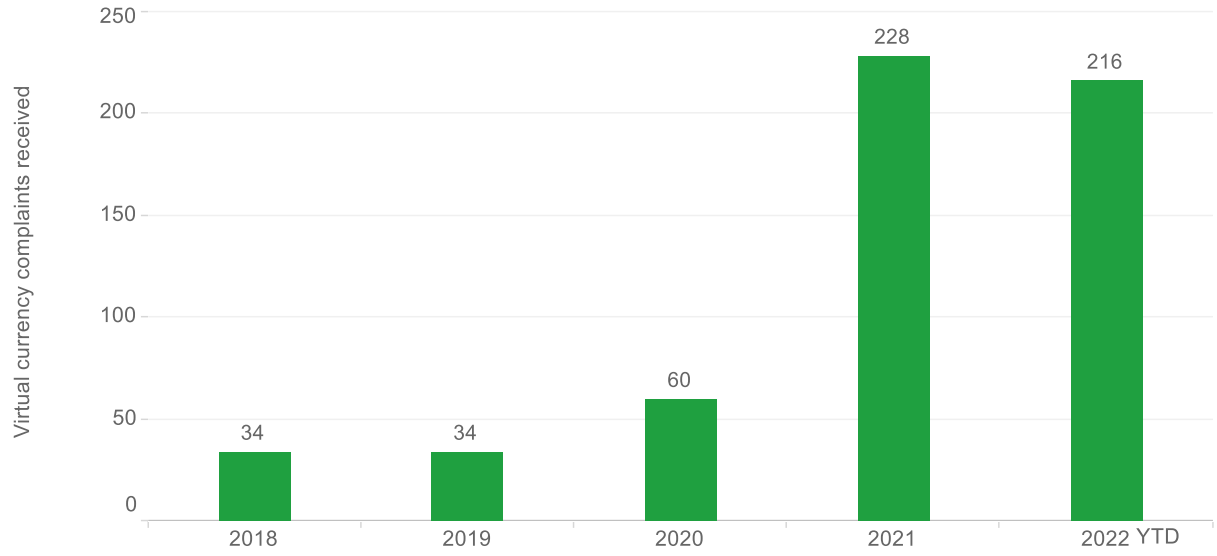
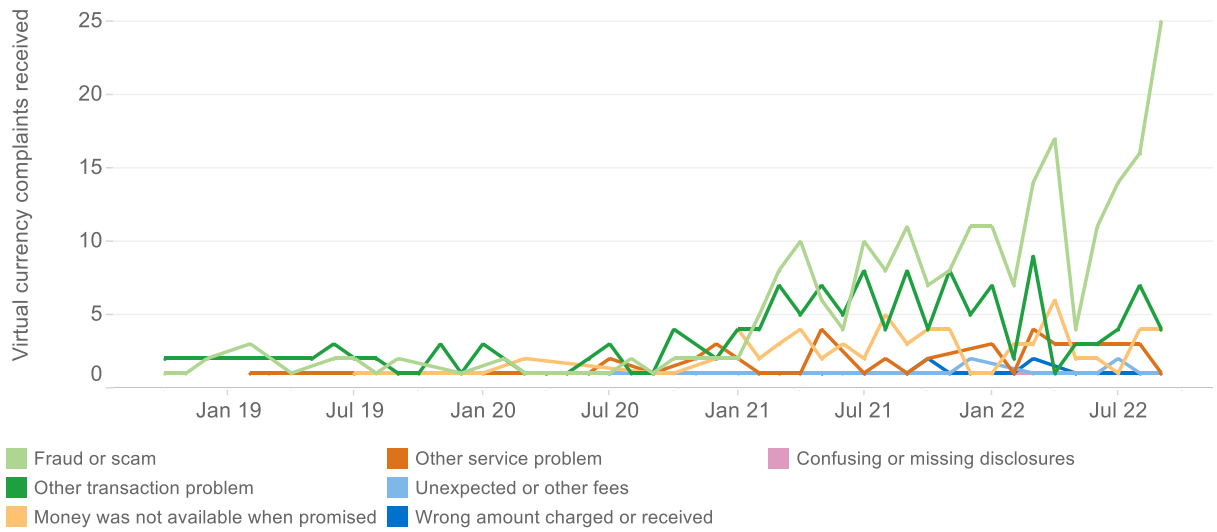


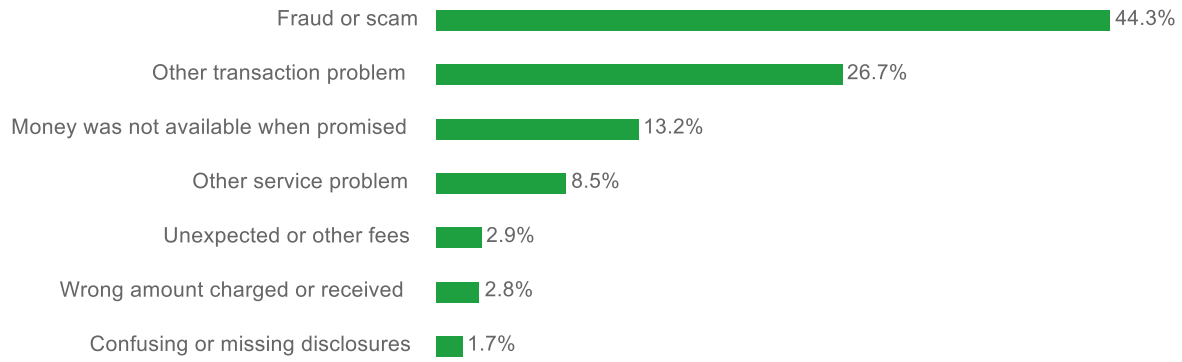
FIGURE 9: VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY OLDER CONSUMERS BY ISSUE OVER TIME, OCT. 2018 TO SEPT. 2022



[84] *See, e.g.,* Fed. Trade Comm'n, *supra* note 1 ("median individual reported losses have tended to increase with age, topping out at $11,708 for people in their 70s").

Of the total virtual currency complaints submitted by older consumers since October 2018, more than 44% were about fraud and scams (Figure 10).

FIGURE 10: VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY OLDER CONSUMERS BY ISSUE, OCT. 2018 TO SEPT. 2022



In one instance, a consumer lost their life savings after two fake customer support scams:

> I have a [crypto-asset] account I have or had over 162,000.00 in it. I was seeking help for a problem [withdrawing crypto-assets from another platform and] the support team there sent me to [a] chat where I was scammed for 5 [crypto-asset] out of my [crypto-asset platform] account …I contacted [the crypto-asset platform support and] I got a case number. Then right after that a thing called Official Support pops up I asked if they were from [the platform], and they said they handle [problems with that platform] …I told them about the scam on the [crypto-asset] and he or she said for me to send them a copy of the withdraw address. I did and they said the [crypto-asset] hasn't made it to the scammer's wallet yet, so I said great can you get it back and they said yes. Well, they even sent me a [official documents from the platform] I had to e-sign saying they could lose the [crypto-asset] in the process. I signed [and] they asked some personal questions. I said I don't know if I should answer, but they keep saying we are the official [platform] support…so I answered them so after a while things goes south they froze my account but keep assuring me it's a part of the process …
>
> Well [in March 2021] I get a email from the bank saying I'm overdrawn on my checking… sure enough someone tried to withdraw 17,900.00 out of my checking [but] the bank stop all but 2500.00 cause that's what I had in it. Anyhow now I felt scammed out of my life savings. I'm 67 and not tech savvy. I don't understand how this could happen…

> Anyhow if you ever dealt with [the platform's customer support, it] is very bad to say the least. After a couple more tries on [date] they answered my account was still frozen I told them the story and I need to check my account they told me its locked cause I owe them money so that told me the scammer took all my money and now I owe [because the platform] has a thing where if you commit to a withdraw from your bank which means a deposit to them you can have the money right away so that's how the scammers got the money from my checking account and since the bank stopped the withdraw cause I couldn't cover it…so now I owe [the platform] money.
>
> So, all I did was went to [the platform's] customer service and put my trust in them [and] I'm out 162,000 plus 17,900 owed to [the platform]. That's 179,900.00. Now I'm 67 with a heart condition and within less than a week I'm broke. Please I'm begging help me I feel [the platform] failed to keep my account secure as no one should go to [the platform] support and have someone help them that's a scammer…[85]

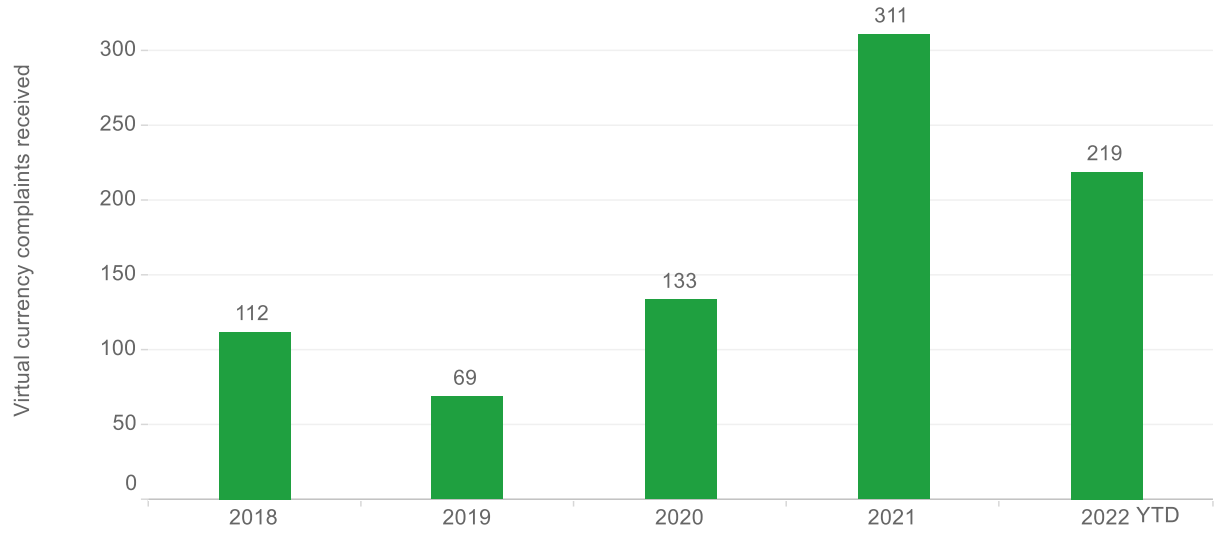
In response, the company stated that the consumer was a victim of a scam, and that the funds were not recoverable.

4.2 Servicemembers

Hundreds of servicemember complaints to the CFPB involved crypto-assets or crypto platforms in the last several years (Figure 11), and complaints include reports of scams targeting servicemembers through identity theft or romance scams.

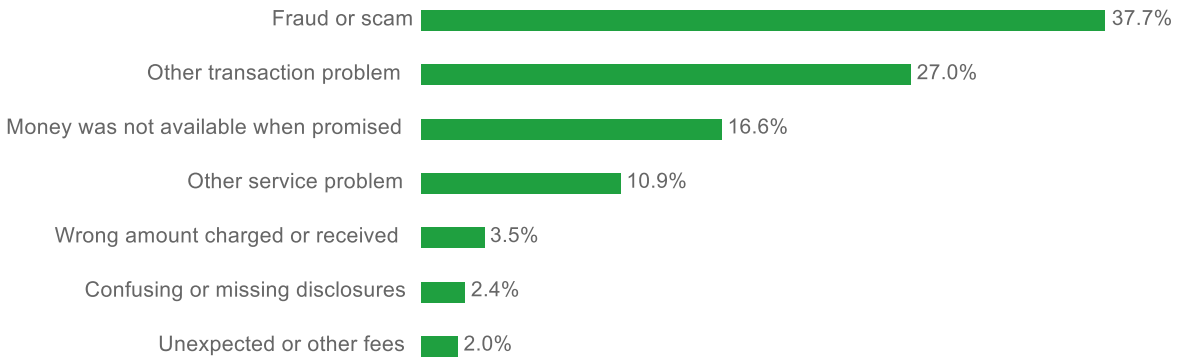
[85] Consumer Complaint 4252242, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4252242.

FIGURE 11: COUNT OF VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY SERVICEMEMBERS, OCT. 2018 TO SEPT. 2022



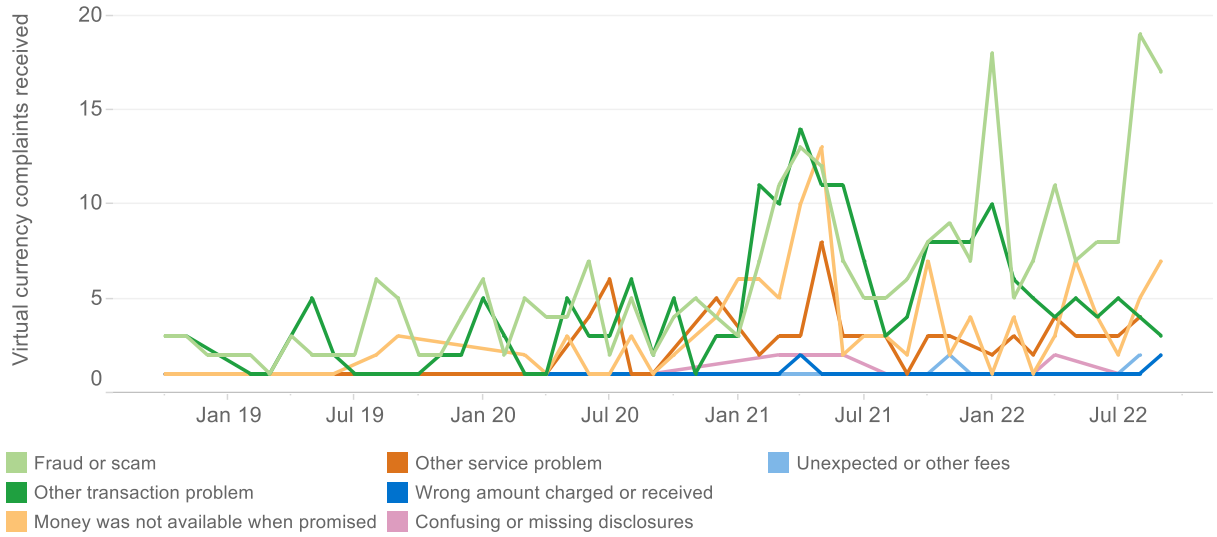
Of the total virtual currency complaints submitted by servicemembers since October 2018, more than 37% were about fraud and scams (Figure 12).

FIGURE 12: VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY SERVICEMEMBERS BY ISSUE, OCT. 2018 TO SEPT. 2022



The CFPB has seen a significant increase in complaints about fraud and scams submitted in the past 12 months (Figure 13). From October 2021, to September 1, 2022, approximately 42% of total virtual currency complaints from servicemembers were about as frauds or scams.

FIGURE 13: VIRTUAL CURRENCY COMPLAINTS SUBMITTED BY SERVICEMEMBERS BY ISSUE OVER TIME, OCT. 2018 TO SEPT. 2022



In one complaint, a servicemember stated that they had lost crypto-assets as the result of identity theft, despite taking extensive steps to stop the fraudulent transactions from taking place:

> I would like to report unauthorized transactions made on my [crypto-asset platform] account. This is to ensure [crypto-asset platform] is advised of all steps taken by me, in an effort to work with [crypto-asset platform] to resolve this matter and regain access to my [crypto-asset platform] account.
>
> [Date]: Text came that my [mobile] password was reset. On [my cell phone], I get text that [crypto-asset platform] password was reset. Asked [cell phone company] for SIM Lock & Port Freeze. [Cell phone company] rep reset my PIN, changed password.
>
> [Date]: Called Internet Service Provider…to change password on email used to login to the T-Mobile and [crypto-asset platform].
>
> [Date]: Received emails from [crypto-asset platform] for following four unauthorized transactions: 1) $104.79, 2) $400.00, 3) $80.63, 4) $35,000.00. I called [crypto-asset platform] … to deactivate my account and completed online form providing details. I received [crypto-asset platform] email …with directions to take security precautions and reply back when ready to restore access to my account. On 4/13/21, I completed all precautions and replied to [crypto-asset platform] to restore access to account.

[Date]: [Bank] shows 2 transactions pending; stop payment on both $400 and $35,000. Changed all banking and credit card passwords.

[Date]: Called [cell phone company]. [Customer service representative] said someone accessed [my] account on 4/12/21, reset password, changed SIM card number within T-[my] account. That allowed criminal to make unauthorized transactions remotely from a new SIM card and phone. [Customer service representative] put port freeze and SIM lock on account.

[Date]: Email response from [crypto-asset platform] state they are working with a specialist to address this issue; to follow-up as soon as they have update.

[Date]: Email from [crypto-asset platform] stated the $35,000.00 and the $400.00 transactions failed. If I don't take action, in 5 days they initiate automatic recovery.

[Date]: I Email [crypto-asset platform] with additional information and request status of their investigation of this issue.

[Date]: I sent online inquiry to [crypto-asset platform] for status update and request account access. They replied by email and have passed all my info on to an account specialist reviewing the case; state it generally takes 4-5 business days.

[Date]: I sent email inquiry to [crypto-asset platform] asking for account specialist to respond with update and help me restore access to my [crypto-asset platform] account.

[Date]: [Officer from county] Sheriff's Department took info and documentation to share with investigators in his office and file police report regarding the unauthorized transactions reported to [crypto-asset platform].

[Date]: I filed identity theft report with the Federal Trade Commission regarding the unauthorized transactions reported to [crypto-asset platform].

[Date]: I sent email inquiry to [crypto-asset platform] asking for account specialist to respond with update and help me restore access to my [crypto-asset platform] account…[86]

[86] Consumer Complaint 4358006, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/4358006.

In response, the company stated that the consumer was a victim of a SIM swap hack. The company also stated that it could not reimburse the consumer, and that the consumer also would need to repay the company over $3500 as a result of the reversed transaction.

5. Discussion

Common among the issues described by consumers in their complaints as discussed in the preceding sections challenges holding companies accountable when consumers experience a problem.

Issue resolution

Consumer complaint outcomes vary widely. In situations where a consumer is facing a technical issue or a problem accessing their account or crypto-assets, they are often able to get the help they need to reestablish access, or at least beginning the process—although as discussed, the wait may be long.

But in situations where consumers have had assets stolen, or had their account hacked, they are often told there is nowhere to turn for help. In one complaint, a consumer reported a loss of their life savings in a scam, which the company stated was not recoverable:

> On [Date], my cell phone, email & [crypto-asset platform] wallet were all hacked.
>
> At around 9:00 PM I turned on my cell phone and realized it wasn't working- I couldn't make any calls and wasn't receiving any messages. When I got in contact with [wireless company] (using my wife's phone), they had advised someone earlier in the day asked to switch the SIM from my iPhone 13 Pro to their iPhone 7…
>
> While on the phone with [wireless company], I had also called [crypto-asset platform] to lock my account. However, the damage was already done. A day later, when I regained access to my [crypto-asset platform] account, I was able to see all the trades this scammer had done…[H]e had sent fractions of the total [crypto-asset] holdings & in 1,000+ (clear fraud & suspicious) transactions sent it all to unknown addresses/ wallets…
>
> Around $70,000 was stolen. The scammer offloaded all the Bitcoin in hundreds of transactions, $15.28 at a time. Isn't it suspicious?? Who would do so many transactions to the same wallet? Isn't it obvious a fraud occurred?

> Below is 1 of 1,000+ transactions [the crypto-asset platform] allowed a scammer to withdraw from my [crypto-asset platform] wallet/ my entire life savings….
>
> [Crypto-asset platform] refuses to help and there's no one to call, "sorry, we can only interact via email." I've sent multiple emails and all they say is "we are looking into it", "there's nothing we can do once the money has left your wallet" and "to call the authorities". I went to the authorities, and they need me to provide the hashtags/ transactions to where the crypto was sent. I asked [crypto-asset platform] to investigate this for me, as I tried every way to do it myself on [crypto-asset platform], and they responded, "that's going to be very hard to do." As to how they let clear fraud and suspicious activity happen is beyond me. But maybe they don't care, as they made a lot of money on these transaction fees. They really need to [be] investigated and held responsible. They do not have proper measures in place and soon enough it's going to happen to many more people…[87]

Fraudulent transactions and platform responses

The complaint above also raises the question of whether crypto-asset platforms are effectively identifying and stopping fraudulent transactions. The pattern mentioned above—hundreds of small transactions to the same wallet—suggests that scammers may be aware of existing controls and purposefully avoiding them. There are Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) obligations under the Bank Secrecy Act required for financial institutions. These obligations include requirements to establish and implement effective, risk-based anti-money laundering programs and recordkeeping and reporting requirements, including the filing of suspicious activity reports (SARs).[88] But as noted by the Department of Justice, there remain significant vulnerabilities: "criminals continue to take advantage of noncompliant actors— including noncompliant cryptocurrency exchanges, peer-to-peer exchangers, or automated cryptocurrency kiosks—to exchange their cryptocurrency for cash or other digital assets without facing rigorous AML/CFT scrutiny."[89]

---

[87] Consumer Complaint 5545300, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5545300.

[88] *See* Joint Statement of Commodity Futures Trading Comm'n, Fin. Crimes Enforcement Network, & U.S. Sec. and Exchange Comm'n, *Leaders of CFTC, FinCEN, and SEC Issue Joint Statement on Activities Involving Digital Assets* (Oct. 11, 2019), https://www.sec.gov/news/public-statement/cftc-fincen-secjointstatementdigitalassets. *See also* Fin. Crimes Enforcement Network, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies (May 9, 2019), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-certain-business-models.

[89] U.S. Dep't of Just., The Role Of Law Enforcement In Detecting, Investigating, And Prosecuting Criminal Activity Related To Digital Assets (Sept. 6, 2022), https://www.justice.gov/ag/page/file/1535236/download.

Some crypto-asset platforms appear only to be taking steps to verify the authority of a person to act on behalf of a customer after receiving a complaint from that customer, and often only after several escalations by that customer.

Crypto-asset platforms sometimes hide behind terms and conditions

In situations where consumers are having problems with a crypto-asset platform or wallet that does not involve fraud or technical issues, companies sometimes cite boilerplate user agreement language to absolve themselves of responsibility.

For example, one consumer complained that their crypto-asset lender blocked access to $18,000 of the consumer's assets due to "liquidity issues." In its response, the company cited its terms of use, which stated in part "that [the company] may experience extreme market conditions which could result in the pausing of withdrawals and transfers between accounts from the user's [account]." The company also directed the consumer to a blog post which stated that the company had "paused all withdrawals and transfers between accounts due to extreme market conditions until further notice."[90] At this writing, withdrawals and transfers are still unavailable at this crypto-asset platform.

Consumers have also submitted complaints, reporting that some crypto-asset platforms have incorporated arbitration clauses into their terms and conditions that requires consumer to resolve disputes through arbitration. For example, according to a consumer:

> Prior to the end of January 2022, I enrolled as a member of a class action lawsuit against [crypto-asset platform] for charging undisclosed transaction fees while advertising no fee transactions. ... At the end of January 2022, [crypto-asset platform] updated its terms of service to require anyone using their site agree to binding arbitration for any disputes between them and a user, past, present, or future. As such, users who are party to the class action are rendered unable to access their accounts in order to download data necessary for income tax reporting without first agreeing to the updated terms of service. This is a flagrantly unconscionable and abusive practice.[91]

Some consumers are bringing actions that are challenging these arbitration clauses.[92]

---

[90] Consumer Complaint 5687115, https://www.consumerfinance.gov/data-research/consumer-complaints/search/detail/5687115.

[91] Consumer Complaint (on file with author).

[92] *See* Bielski v. Coinbase, Inc., No. C 21-07478 WHA, 2022 WL 1062049 (civil action against a crypto-asset platform in which the court denied the platform's motion to compel arbitration).

6. Consumer risks and resources

Generally, providers of consumer financial products and services offering crypto-assets and related services, and consumers who want to use crypto-assets should remember some key facts and risks. There are also some steps consumers can take to protect themselves.

Key facts and risks

- **Crypto-assets are a common target for hacking.** Crypto platforms are a frequent target of hacks by malicious actors, including certain nation-state actors. Hackers affiliated with one nation state have stolen over $2 billion in crypto-assets total,[93] including more than $1 billion from Jan 2022 to July 2022 alone,[94] and their hacks have included several prominent crypto platforms, including a "play to earn" crypto-asset game.[95] The top 10 crypto-asset hacks alone have amounted to over $2.5 billion in losses from August 2021 to November 2022 according to one industry report.[96]
- **Important terms and clarifications are often buried in the Terms and Conditions:** It is important that consumers read the agreement between them and their wallet provider and crypto-asset platform (often found under "Terms and Conditions" sections). If questions arise as to what rights you may have under the agreement, reach out to the wallet provider or crypto-asset platform for a written answer.
- **Arbitration clauses and class action bans may limit dispute options.** Many crypto-asset platforms and associated service providers use dispute resolution

[93] *See, e.g.,* Elliptic Connect, *supra* note 3.

[94] *See, e.g.,* Choe Sang-Hun and David Yaffe-Bellany, *supra* note 4.

[95] *See* Statement, Fed. Bureau of Investigation, *supra* note 5. *See also* Aaron Schaffer, *supra* note 5.

[96] Rekt News, Leaderboard, https://rekt.news/leaderboard/.

mechanisms such as mandatory arbitration clauses and class action bans that inhibit consumers' and investors' ability to pursue legal claims.[97]

- **The value of crypto-assets have and will likely continue to fluctuate greatly.** It is important that consumers be aware of the risk of financial loss when acquiring crypto-assets. Consumers have reported losing their savings after acquiring crypto-assets because the value decreased significantly.
- **Transactions may not be as private as imagined.** Many crypto-asset transactions are recorded on publicly accessible blockchains, and those transactions are associated with a crypto-asset address. People with the correct knowledge and motivation maybe be able to link those transactions and the crypto address with a consumer's identity or their other transactions. In addition, in the bankruptcy proceeding of one crypto-asset platform, the names and recent transactions of all customers were published.[98]
- **The use of crypto-assets may violate sanctions**. On certain blockchains, a consumer's transaction may be validated by an anonymous entity and/or a sanctioned person, as blockchain users cannot choose their miner or validator.[99]

Steps consumers can take to protect themselves

- **Watch out for signs of a scam.** Beware of claims promising huge rates of return. No legitimate government or business will require a consumer to buy crypto-assets. If they do, it is a scam.[100]
- **Don't mix crypto-assets and romance.** Consumers should be very careful if a new love interest, especially one they have never met in person, wants to show them how to invest in crypto-assets or asks them to send crypto. It is probably a scam.[101]
- **Know who you are dealing with.** Consumers should make sure they know how to contact the platform if something goes wrong with a crypto-asset transaction. Some

---

[97] U.S. Dep't of the Treasury, *supra* note 10 at 33.

[98] *See, e.g.,* Matt Novak, *Celsius Execs Cashed out at Least $17 Million in Crypto Before Halting Withdrawals for Customers*, Gizmodo (Oct. 6, 2022), https://gizmodo.com/celsius-execs-cashed-out-bitcoin-price-crypto-ponzi-1849623526.

[99] Fin. Stability Oversight Council, *supra* note 6 at 44.

[100] *See, e.g.,* Consumer Fin. Prot. Bureau, Fraud and scams, https://www.consumerfinance.gov/consumer-tools/fraud/.

[101] *See, e.g.,* Consumer Fin. Prot. Bureau, Money Smart for Older Adults: avoid financial exploitation, https://www.consumerfinance.gov/consumer-tools/educator-tools/resources-for-older-adults/money-smart-for-older-adults.

crypto-asset platforms do not identify their owners, their phone numbers and addresses, or even the countries where they are located.

- **Understand what the actual costs will be.** Know the relevant exchange rate and how it was determined. Find out in advance about mark-ups to the exchange rate or other fees. Find out how long the transaction will take to complete.
- **Access resources.** Both the CFPB and the FTC offer online resources to help consumers spot and avoid crypto-asset scams and theft. The FTC has published an online guide titled "What to Know About Cryptocurrency and Scams," while the CFPB released the consumer advisory "Risks to consumers posed by virtual currencies."
- **Report any suspicious claims of FDIC insurance.** If crypto-asset or other firms misuse the name or logo of the FDIC or engage in false advertising or make misrepresentations to consumers about deposit insurance, it likely violates the Consumer Financial Protection Act's prohibition on deception, whether or not such conduct is engaged in knowingly.[102] If consumers suspect a platform may be making false claims about FDIC insurance, they can submit a complaint to the CFPB.
- **Submit a complaint to the CFPB.** If consumers have a problem with a consumer financial product or service, they can submit a complaint online or by calling (855) 411-2372.

[102] Consumer Fin. Prot. Bureau, Consumer Financial Protection Circular 2022-02: Deceptive representations involving the FDIC's name or logo or deposit insurance, https://www.consumerfinance.gov/compliance/circulars/circular-2022-02-deception-representations-involving-the-fdics-name-or-logo-or-deposit-insurance/.