Consumer Protection Data Spotlight

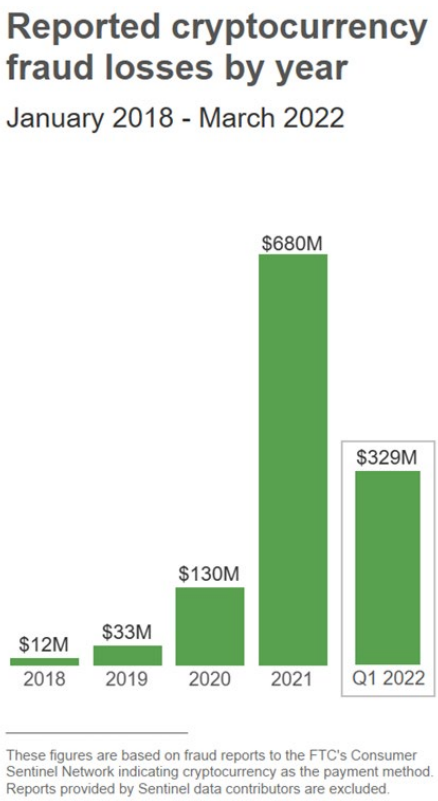
FTC reporting back to you

Reports show scammers cashing in on crypto craze

From Super Bowl ads to Bitcoin ATMs, cryptocurrency seems to be everywhere lately. Although it's yet to become a mainstream payment method, reports to the FTC show it's an alarmingly common method for scammers to get peoples' money. Since the start of 2021, more than 46,000 people have reported losing over $1 billion in crypto to scams[1] – that's about one out of every four dollars reported lost,[2] more than *any* other payment method. The median individual reported loss? A whopping $2,600. The top cryptocurrencies people said they used to pay scammers were Bitcoin (70%), Tether (10%), and Ether (9%).[3]

Crypto has several features that are attractive to scammers, which may help to explain why the reported losses in 2021 were nearly *sixty times* what they were in 2018. There's no bank or other centralized authority to flag suspicious transactions and attempt to stop fraud before it happens. Crypto transfers can't be reversed – once the money's gone, there's no getting it back. And most people are still unfamiliar with how crypto works. These considerations are not unique to crypto transactions, but they all play into the hands of scammers.

Reports point to social media and crypto as a combustible combination for fraud. Nearly half the people who reported losing crypto to a scam since 2021 said it started with an ad, post, or message on a social media platform.[4] During this period, nearly four out of every ten dollars reported lost to a fraud originating on social media was lost in crypto, far more than any other payment method.[5] The top platforms identified in these reports were Instagram (32%), Facebook (26%), WhatsApp (9%), and Telegram (7%).[6]



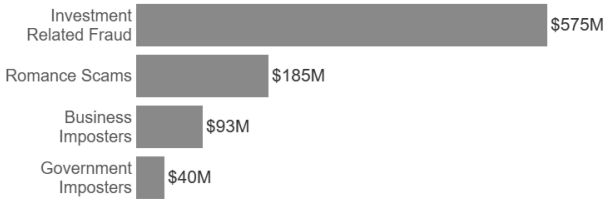
Of the reported crypto fraud losses that began on social media, most are investment scams.[7] Indeed, since 2021, $575 million of all crypto fraud losses reported to the FTC were about bogus investment opportunities, far more than any other fraud type. The stories people share about these scams describe a perfect storm: false promises of easy money paired with people's limited crypto understanding and experience. Investment scammers claim they can quickly and easily get huge returns for investors. But those crypto "investments" go straight to a scammer's wallet. People report that investment websites and apps let them track the growth of their crypto, but it's all fake. Some people report making a small "test" withdrawal – just enough to convince them it's safe to go all in. When they really try to cash out, they're told to send *more* crypto for (fake) fees, and they don't get any of their money back.

Romance scams are a distant second to investment scams, with $185 million in reported cryptocurrency losses since 2021 – that's nearly one in every three dollars reported lost to a romance scam during this period.[8] And many have an investment twist too. These keyboard Casanovas reportedly dazzle people with their supposed wealth and sophistication. Before long, they casually offer tips on getting started with crypto investing and help with making investments. People who take them up on the offer report that what they really got was a tutorial on sending crypto to a scammer. The median individual reported crypto loss to romance scammers is an astounding $10,000.

Business and government impersonation scams are next with $133 million in reported crypto losses since 2021. These scams can start with a text about a supposedly unauthorized Amazon purchase, or an alarming online pop-up made to look like a security alert from Microsoft. From there, people are reportedly told the fraud is extensive and their money is at risk. The scammers may even get the "bank" on the line to back up the story. (Pro tip: it's not the bank.) In another twist, scammers impersonating border patrol agents have reportedly told people their accounts will be frozen as part of a drug trafficking investigation. These scammers tell people the only way to protect their money is to put it in crypto: people report that these "agents" direct them to take out cash and feed it into a crypto ATM. The "agent" then sends a QR code and says to hold it up to the ATM camera. But that QR code is embedded with the scammer's wallet address. Once the machine scans it, their cash is gone.

Top frauds by reported cryptocurrency losses

January 2021 - March 2022



These figures are based on fraud reports to the FTC's Consumer Sentinel Network indicating cryptocurrency as the payment method. The investment related fraud category includes the following fraud subcategories: art, gems and rare coin investments, investment seminars and advice, stocks and commodity futures trading, and miscellaneous investments. Reports provided by Sentinel data contributors are excluded.

People ages 20 to 49 were more than *three times* as likely as older age groups to have reported losing cryptocurrency to a scammer.[9] Reports point to people in their 30s as the hardest hit – 35% of their reported fraud losses since 2021 were in cryptocurrency.[10] But median individual reported losses have tended to increase with age, topping out at $11,708 for people in their 70s.[11]

Here are some things to know to steer clear of a crypto con:

- **Only scammers will guarantee profits or big returns.** No cryptocurrency investment is ever guaranteed to make money, let alone big money.
- **Nobody legit will require you to buy cryptocurrency.** Not to sort out a problem, not to protect your money. That's a scam.
- **Never mix online dating and investment advice**. If a new love interest wants to show you how to invest in crypto, or asks you to send them crypto, that's a scam.

To learn more about cryptocurrency scams – and how to spot and avoid scams generally – visit ftc.gov/cryptocurrency and ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

The FTC uses reports from the public to investigate and stop fraud, for consumer education and outreach, and for analyses like this. File your fraud report at ReportFraud.ftc.gov. To explore Sentinel data, visit FTC.gov/exploredata.

1 These figures and figures throughout this Spotlight, unless otherwise noted, are based on fraud reports made directly to the FTC in the Consumer Sentinel Network database from January 1, 2021 through March 31, 2022 that indicated cryptocurrency as the payment method. Reports provided by Sentinel data contributors are excluded because of inconsistencies among contributors in capturing payment information. Because the vast majority of frauds are not reported, these figures reflect just a small fraction of the public harm. *See* Anderson, K. B., *To Whom Do Victims of Mass-Market Consumer Fraud Complain?* at 1 (May 2021), *available at* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852323 (study showed only 4.8% of people who experienced mass-market consumer fraud complained to a Better Business Bureau or a government entity).

2 From January 1, 2021 through March 31, 2022, cryptocurrency was identified as the payment method for 24% of reported dollar losses in fraud reports to the FTC.

3 These figures exclude reports that did not specify the type of cryptocurrency.

4 From January 1, 2021 through March 31, 2022, 49% of fraud reports to the FTC indicating cryptocurrency as the payment method specified that the scam started on social media, compared to 37% in 2020, 18% in 2019, and 11% in 2018.

5 From January 1, 2021 through March 31, 2022, $1.1 billion was reported to the FTC as lost to fraud originating on social media. Of that number, 39% was reported as paid using cryptocurrency, followed by bank transfer or payment (20%), and wire transfer (9%). 8% did not indicate a payment method.

6 These figures exclude reports that did not specify a social media platform.

7 From January 1, 2021 through March 31, 2022, people reported to the FTC that $417 million in cryptocurrency was lost to fraud originating on social media. $273 million of these losses were to fraud categorized as investment related, followed by romance scams ($69 million), and business imposters ($35 million).

8 From January 1, 2021 through March 31, 2022, cryptocurrency was identified as the payment method for 29% of reported dollar losses to romance scams.

9 From January 1, 2021 through March 31, 2022, people ages 20 to 49 submitted fraud loss reports to the FTC indicating social media as the contact method at a rate 3.4 times greater than people 50 and over. About 91% of fraud reports indicating cryptocurrency as the payment method during this period included age information. This age comparison is normalized based on the number of loss reports per million population by age during this period. Population numbers were obtained from the U.S. Census Bureau Annual Estimates of the Resident Population for Selected Age Groups by Sex for the United States (June 2020).

10 From January 1, 2021 through March 31, 2022, the percentage of total reported fraud losses that were lost in cryptocurrency by age were as follows: 12% (18-19), 23% (20-29), 35% (30-39), 33% (40-49), 28% (50-59), 19% (60-69), 10% (70-79), and 2% (80 and over). These figures exclude reports that did not indicate age.

11 From January 1, 2021 through March 31, 2022, the median individual reported cryptocurrency losses to fraud by age were as follows: $1,000 (18-19), $1,600 (20-29), $2,500 (30-39), $3,200 (40-49), $5,000 (50-59), $8,500 (60-69), $11,708 (70-79), and $8,100 (80 and over).