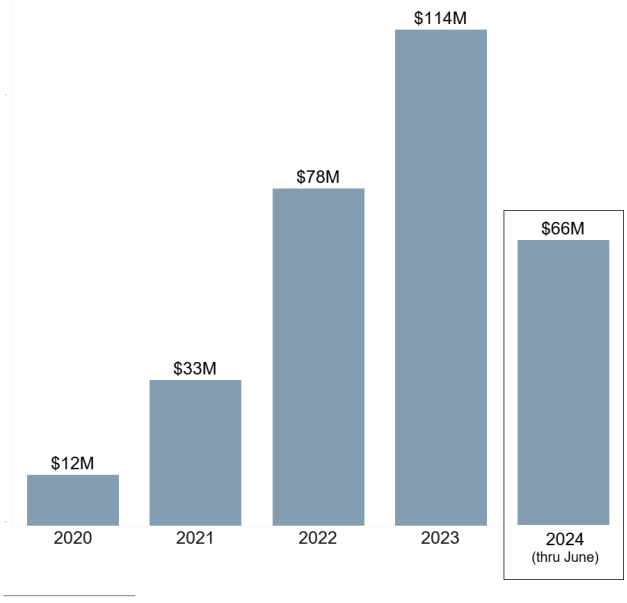
Consumer Protection Data Spotlight
FTC reporting back to you

Bitcoin ATMs: A payment portal for scammers

Bitcoin ATMs (or BTMs)[1] have been popping up at convenience stores, gas stations, and other high-traffic areas for years.[2] For some, they're a convenient way to buy or send crypto, but for scammers they've become an easy way to steal. FTC Consumer Sentinel Network data show that fraud losses at BTMs are skyrocketing, increasing nearly tenfold from 2020 to 2023, and topping $65 million in just the first *half* of 2024.[3] Since the vast majority of frauds are not reported, this likely reflects only a fraction of the actual harm.[4]

Reported BTM fraud losses by year

January 2020 - June 2024



These figures are estimates based on keyword analysis of the narratives provided in reports to the FTC's Consumer Sentinel Network that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used. The estimated number of reports by year are as follows: 902 (2020), 1,981 (2021), 3,698 (2022), 4,863 (2023), and 2,968 (through June 2024).

Cryptocurrency surged as a major payment method for scams in recent years, along with the massive growth in crypto payments on fake investment opportunities.[5] But now crypto is a top payment method for many other scams, too.[6] Widespread access to BTMs has helped make this possible. Reports of losses using BTMs are overwhelmingly about government impersonation, business impersonation, and tech support scams.[7] And when people used BTMs, their reported losses are exceptionally high. In the first six months of 2024, the median loss people reported was $10,000.[8]

In the first half of the year, people 60 and over were more than three times as likely as younger adults to report a loss using a BTM.[9] In fact, more than two of every three dollars reported lost to fraud using these machines was lost by an older adult.[10]

Scams that use BTMs work in lots of different ways. Many start with a call or message about supposed suspicious activity or unauthorized charges on an account.[11] Others get your attention with a fake security warning on your computer, often impersonating a company like Microsoft or Apple. These things are hard to ignore, and that's the point. From there, the story quickly escalates. They might say all your money is at risk, or your information has been linked to money laundering or even drug smuggling. The scammer may get a fake government agent on the line – maybe even claiming to be from the "FTC" – to up the ante.

So where do BTMs fit into the story? Scammers claim that depositing cash into these machines will protect your money or fix the fake problem they've concocted. They've even called BTMs "safety lockers." They direct you to

go to your bank to take out cash. Next, they send you to a nearby BTM location – often a specific one – to deposit the cash you just took out of your bank account.[12] They text you a QR code to scan at the machine, and once you do, the cash you deposit goes right into the scammer's wallet.

So how can you spot and steer clear of these scams?

- Never click on links or respond directly to unexpected calls, messages, or computer pop-ups. If you think it could be legit, contact the company or agency, but look up their number or website yourself. Don't use the one the caller or message gave you.
- Slow down. Scammers want to rush you, so stop and check it out. Before you do anything else, talk with someone you trust.
- Never withdraw cash in response to an unexpected call or message. Only scammers will tell you to do that.
- Don't believe anyone who says you need to use a Bitcoin ATM, buy gift cards, or move money to protect it or fix a problem. Real businesses and government agencies will never do that – and anyone who asks is a scammer.

To spot and avoid scams visit ftc.gov/scams. Report scams to the FTC at ReportFraud.ftc.gov.

1 While machines that allow consumers to buy cryptocurrency are commonly referred to as Bitcoin ATMs or BTMs, these machines often handle – and scams can take place in – other cryptocurrencies in addition to Bitcoin.

2 BTM installations self-reported by operators to an industry website increased from about 4,250 in January 2020 to about 32,000 in June 2024. See trend chart available at https://coinatmradar.com/charts/growth/united-states/.

3 These and other figures throughout this Spotlight are estimates based on keyword analysis of the narratives provided in reports that identified cryptocurrency as the payment method. Not all reports identify a payment method or include sufficient details in the report narrative to determine whether a BTM was used.

4 *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).

5 See FTC Consumer Protection Data Spotlight, *Reports Show Scammers Cashing in on Crypto Craze* (June 3, 2022), available at https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2022/06/reports-show-scammerscashing-crypto-craze.

6 In the first half of 2024, cryptocurrency was the top payment method in terms of aggregate reported losses on tech support scams and job scams, and the second most costly method after bank transfers on business impersonation scams, government impersonation scams, romance scams, and family and friend impersonation scams.

7 In the first half of 2024, about 86% of people who reported a fraud loss using a BTM indicated that it was on a government impersonation, business impersonation, and/or tech support scam. This excludes reports categorized as unspecified.

8 In the first half of 2024, the median individual reported fraud loss when cryptocurrency was the reported payment method (including reports with and without BTM use) was $5,400; the median individual reported loss to fraud generally was $447.

9 This comparison of older and younger consumers' reporting rates is normalized based on the population size of each age group using the Census Bureau's 2018-2022 American Community Survey 5-Year Estimates. This excludes reports that did not include consumer age information.

10 In the first half of 2024, people 60 and over reported losing $46 million using BTMs, or about 71% of the reported losses using these machines. During the same period, when a reported cryptocurrency fraud loss did *not* involve the use of a BTM, about 72% of the losses were reported by people 18 to 59. Most of these losses were to fake cryptocurrency investment opportunities. Percentage calculations exclude reports that did not include consumer age information.

11 Phone calls were the initial contact method in about 47% of these reports, followed by online ads or pop-ups (16%), and e-mails (9%). Reports indicating online ad or pop-up as the contact method typically described fake computer security alerts. People reported that security pop-ups and email messages included a phone number to call for help.

12 Reports show that scammers direct people to specific BTM locations and many consumers name the BTM operator in their reports. These details show a pattern that suggests scammers prefer some operators over others and that these preferences have changed over time. While the reports do not tell us why this might be, differences in fraud prevention measures taken by various operators likely play a role.