CRYPTOCURRENCY INVESTMENT SCAM

Cryptocurrency investment scams have emerged as one of the most damaging consumer scam types. These scams often begin with an ad, post or message on social media soliciting interest in a "no-risk, guaranteed high-return" investment opportunity in cryptocurrency. Potential victims also may be targeted by criminals posing as investment managers or prospective romantic interests on dating websites. In these instances, the criminal builds trust with the victim, offers to share some investing advice, and persuades them to deposit money into proposed cryptocurrency "investments." The criminal then tricks the victim into believing that they received a high return on their initial investment (e.g., showing them a fake account balance), which encourages them to deposit increasing amounts of money. In reality, that money was stolen by the criminal. The victim typically loses all the money they "invested," with often devastating financial and emotional impacts.

Refer to page 2 for a cryptocurrency scam example.

CRYPTOCURRENCY INVESTMENT SCAM

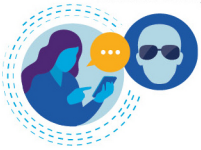
1. Joanne joins a dating app hoping to discover a new love interest. She matches with John, who is living overseas.

2. Joanne and John begin a long-distance romance, chatting and sending emails to each other daily.

3. Some months pass. John tells Joanne about a new low-risk, high-return investment opportunity in cryptocurrency. He claims he had a 250% return on this investment in the past year.

4. Joanne is skeptical. She is less familiar with cryptocurrency and has read media reports about get-rich-quick schemes.

5. John shows Joanne his growing crypto account balances over the last few months. He says she should invest quickly because these types of returns are unlikely to last much longer. This persuades Joanne to make a small $2,000 initial investment.



6. Joanne observes a 50% return in just a few weeks. In the next two months, she makes increasingly large additional deposits totaling $42,000.

7. Joanne tries to withdraw cash from her crypto account to pay for unexpected medical bills. She is surprised that she is unable to do so.

8. Joanne contacts John for help but he doesn't respond. She is devastated to realize the investment opportunity was a scam. She contacts her financial institution and law enforcement.

The scams mitigation toolkit was developed by the Federal Reserve to help educate the industry about scams and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.