

## **Beware of Cryptocurrency Payment Scams**

Beware! A request for payment in cryptocurrency is a sure sign of a scam. Like most payment scams, someone will contact you pretending to be from the government, law enforcement, a local utility company, a lottery prize promoter, or even your bank. They will fabricate a story that gains your trust and motivates you to make a payment. For example, they will convince you that they represent your utility company and if you do not make payment immediately your utilities will be turned off. Once you agree to make payment, they will direct you to withdraw cash from your bank, investment, or retirement accounts, go to a store with a cryptocurrency ATM, insert your cash into the ATM, and buy cryptocurrency. The scammer will then send you a QR code that includes their address and have you scan the QR code so the money gets transferred to them. Once it's transferred the cryptocurrency is lost and your money CANNOT be recovered.



- The government, law enforcement, utility companies, prize promotors, banks, and any other legitimate vendors will NEVER ask you to pay with cryptocurrency.
- Unexpected calls, texts, social media messages, or tweets asking you to pay for something with cryptocurrency IS A SCAM.
- Always do thorough research with a trusted source before investing in cryptocurrencies. Cloned websites or misspellings on websites are signs of a scam.

## How To Report Cryptocurrency Scams:

- the FTC at <u>ReportFraud.ftc.gov</u>
- the Commodity Futures Trading Commission (CFTC) at <u>CFTC.gov/complaint</u>
- the U.S. Securities and Exchange Commission (SEC) at <u>sec.gov/tcr</u>

For more information about avoiding cryptocurrency scams, visit <u>ftc.gov/cryptocurrency</u>

If you have any questions, please call our Customer First Contact Center at (203) 462-4400 (Monday – Friday (excluding bank holidays) from 8:30 a.m. to 4:30 p.m.)

> March 9, 2022 Member FDIC

NMLS # 411487