# MARYLAND COMMISSIONER OF FINANCIAL REGULATION

# CONSUMER ADVISORY

**December 18, 2023**

## Avoid Scams Involving Cryptocurrency ATMs

Protect yourself and your loved ones from financial fraud and scams involving cryptocurrency and virtual currency ATMs. Recent reports show that scammers are stealing large sums of money from unsuspecting consumers by directing their victims to use cryptocurrency ATMs.

Generally speaking, once cryptocurrency is sent, the transaction cannot be canceled, reversed or refunded. This advisory provides information about the common tactics fraudsters use to scam victims and how you can protect yourself from fraud.

### Common Cryptocurrency ATM Scams

Cryptocurrency ATMs – also known as virtual currency kiosks or Bitcoin ATMs – look and operate like bank ATMs. Fraudsters make contact with unsuspecting consumers and create a sense of urgency in order to convince them to withdraw cash from their bank account and use that cash to purchase virtual currency through a cryptocurrency ATM. The money from the purchase of the cryptocurrency is then sent to the scammer's crypto wallet. Some of the common tactics used by scammers include:

- **Pig Butchering Scams**: "Pig butchering" scams resemble the practice of fattening a hog before slaughter. The fraudsters develop fake identities and "fatten" up the victim by making them believe they are in a trusted relationship before stealing the victim's money. "Pig butchering" scams often begin with the scammer making initial contact with the victim through text messages, social media, or other communication platforms. After developing a fictitious relationship, the scammer presents a cryptocurrency investment opportunity. The scammer then convinces the victim to "invest" cash using a cryptocurrency ATM with instructions to send cryptocurrency to an "investment site", which is actually the scammer's crypto wallet. The Financial Crimes Enforcement Network (FinCEN) recently issued an alert with more information about this scam.

- **Romance Scams**: In a romance scam, the scammer finds and contacts someone through dating websites, apps, or social media. Over time, the scammer gains the victim's trust and makes the victim believe that they are involved in a romantic relationship. The scammer will eventually ask the victim for money, usually for assistance with an emotionally-charged issue like a falsified medical or travel emergency. The scammer convinces the victim to send the money using a cryptocurrency ATM.

- **Impersonation Scams:** The fraudster will impersonate an official from a government agency, such as law enforcement, the Internal Revenue Service (IRS) or the Social Security Administration, or they will pretend to be from a utility company. The scammer may threaten the victim with jail time or with shutting off their electric or other utility services over an alleged unpaid debt. The fraudster uses threats to create fear in the victim and ultimately convince them to deposit cash in a cryptocurrency ATM.

- **Computer "Anti-Virus Protection" Scams:** This scam occurs when a victim sees a "pop up" alert on their computer instructing them to call a "help desk" number to receive anti-virus protection. The victim calls the number and during the call, the victim is told that hackers gained unauthorized access to the victim's bank account, and that they need to convert their cash to cryptocurrency using a cryptocurrency ATM.

## General Tips to Avoid Scams

Scammers are always creating new schemes to defraud victims. Do not make any payments using cryptocurrency out of pressure from, or fear of, someone you do not know. If a call, text, message or request seems random or unusual, do not respond to it.

Here are additional tips to avoid becoming a victim of a scam involving cryptocurrency ATMs:

- Do not pay anyone who contacts you and demands advance payment in cryptocurrency, including through the use of an ATM.
- Be suspicious of unsolicited communications. If you receive an unsolicited call or text message, it may be from a scammer.
- If someone claims to be from a company or government agency and requests a payment, hang up and call back using the customer service number published on their website.
- Do not share your personal information or financial details or give access to your accounts without verifying who you are communicating with.

Learn more about the risks of cryptocurrency here.

## Report Scams and Fraud

**It is important that you report scams and instances of suspected fraud.** If you are the victim of a scam involving a cryptocurrency ATM, you may file a consumer complaint with our Office and we will investigate the operator of the ATM. You should also notify the financial institution which holds the account where your funds have been withdrawn to pay for the cryptocurrency – your financial institution may conduct their own investigation.

Additionally, you may file a report with the following federal agencies for investigation and assistance:

- FBI's Internet Crime Complaint Center (IC3): https://www.ic3.gov/
- Securities and Exchange Commission: https://www.sec.gov/tcr
- If you are an elderly victim or assisting an elderly victim, call the Department of Justice's National Elder Fraud Hotline at 1-833-FRAUD11 or 1-833-372-8311.

---

*The Office of Financial Regulation, a division of the Maryland Department of Labor, is Maryland's consumer financial protection agency and financial services regulator. For more information, please visit our website at www.labor.maryland.gov/finance.*

Maryland
DEPARTMENT OF LABOR
Office of Financial Regulation

**Click here to subscribe to emails from the Office of Financial Regulation.**
Please save "md-dllr-ocfr@info.maryland.gov" in your email contacts to help prevent Office communications from being blocked by your email provider's security features.