MARYLAND COMMISSIONER OF FINANCIAL REGULATION

INDUSTRY ADVISORY REGULATORY ALERT

February 27, 2024

Alert on Scams Involving Cryptocurrency ATMs

The Office of Financial Regulation (OFR) is issuing this alert to Maryland chartered banks and credit unions to highlight recent scams involving cryptocurrency and virtual currency automated teller machines (ATMs). Recent reports show that scammers are stealing large sums of money from unsuspecting consumers by directing their victims to use cryptocurrency ATMs.

This advisory provides information about the common tactics fraudsters use to scam victims. The advisory also includes ways banks and credit unions can detect suspicious activity relating to cryptocurrency ATM scams and methods to better protect their customers and members from fraud.

Common Cryptocurrency ATM Scams

Cryptocurrency ATMs – also known as virtual currency kiosks or Bitcoin ATMs – look and operate like bank ATMs. Fraudsters contact 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 secretly 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. Also, the fraudster will impersonate an employee of a bank or credit union's fraud department telling the victim that fraudulent activity has been detected in their account(s) and that they need to withdraw the funds from their account(s) and deposit the money in a cryptocurrency ATM. 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.

- **Email Scams:** The fraudster will compromise a customer's email account and gain access to their computer through fraudulent links, pop-ups, attachments, surveys, etc. (i.e., anything can be used with the goal being to get the customer to click on something or open something). Once the fraudster has control of the customer's computer, and the customer can see the fraudster moving the cursor and operating their computer, the victim is told to withdraw funds from their bank account(s) and deposit the money in a cryptocurrency ATM (paying the ransom) in order to get their computer back.

Detecting, Preventing and Reporting Suspicious Activity

The following red flags may help banks and credit unions detect and prevent suspicious activity involving cryptocurrency ATMs:

- A customer with no prior history of using or purchasing cryptocurrency suddenly attempts to exchange a significant amount of cash from their account for cryptocurrency.
- A customer expresses interest in an investment opportunity involving cryptocurrency that they recently learned about from an unknown person that reached out to them online or through a text message.
- A customer mentions that they were instructed by an unknown person who reached out to them to exchange cash for cryptocurrency at a cryptocurrency ATM and to deposit the cryptocurrency at a specific address.
- A customer seems stressed or anxious about withdrawing funds in order to make a transaction involving cryptocurrency.
- A customer unusually and prematurely liquidates their savings account(s) and then attempts to wire the liquidated funds or exchange the funds for cryptocurrency.
- A customer takes out a Home Equity Loan (HELOC), or second mortgage and uses the proceeds to purchase cryptocurrency.
- Inactive accounts suddenly show unusual and frequent cash withdrawals of large amounts that are subsequently wired or exchanged for cryptocurrency.
- System monitoring shows that a customer's account (including their online account) is frequently accessed by different IP addresses, device IDs, geographies, or names inconsistent with the customer's typical logins.

FinCEN advises that banks and credit unions file a Suspicious Activity Report (SAR) if they see any red flags or indicators suggesting that their customer may have been defrauded in connection with a cryptocurrency ATM. Banks and credit unions can learn more about pig-butchering scams and other red flags and indicators, as well as how to file a SAR, here.

Contact

For questions, please contact Assistant Commissioner Shereefat Balogun by phone at 410-230-6390, or by email at shereefat.balogun@maryland.gov.

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.