Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

November 04, 2021

Alert Number
I-110421-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations:
www.fbi.gov/contact-us/field-offices

The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

The FBI warns the public of fraudulent schemes leveraging cryptocurrency ATMs and Quick Response (QR) codes to facilitate payment. The FBI has seen an increase in scammers directing victims to use physical cryptocurrency ATMs and digital QR codes to complete payment transactions.

A QR code is a square barcode with information that can be scanned and read with a smartphone camera. An individual can scan the QR code of an intended recipient to auto-populate the recipient field making it easier to send cryptocurrency to the correct destination. QR codes can be used at cryptocurrency ATMs to direct payment to an intended recipient. While many businesses have legitimately used QR code payment in the last year because of the COVID-19 pandemic, QR codes also play a role in malicious use of cryptocurrency payments.

Criminal actors, in various fraudulent schemes, maliciously leverage cryptocurrency ATMs and QR codes to receive payments from victims. Such schemes include online impersonation schemes (scammer falsely identifies as a familiar entity such as the government, law enforcement, a legal office, or a utility company), romance schemes (scammer establishes an online

relationship with a victim by creating a false sense of intimacy and dependency), and lottery schemes (scammer falsely convinces a victim that they have won an award and consequently demands the victim to pay lottery fees).

Regardless of the scheme, the methods using cryptocurrency ATMs and QR codes appear similar. The scammer often requests payment from the victim and may direct the victim to withdraw money from the victim's financial accounts, such as investment or retirement accounts. The scammers provide a QR code associated with the scammer's cryptocurrency wallet for the victim to use during the transaction. The scammer then directs the victim to a physical cryptocurrency ATM to insert their money, purchase cryptocurrency, and use the provided QR code to auto-populate the recipient address. Often the scammer is in constant online communication with the victim and provides step-by-step instructions until the payment is completed.

Cryptocurrency's decentralized nature creates challenges that makes it difficult to recover. Once a victim makes the payment, the recipient instantly owns the cryptocurrency, and often immediately transfers the funds into an account overseas. This differs from traditional bank transfers or wires where a payment transaction can remain pending for one to two days before settlement. It can also make law enforcement's recovery of the funds difficult and can leave many victims with a financial loss.

Tips to Protect Yourself:

- Do not send payment to someone you have only spoken to online, even if you believe you have established a relationship with the individual.
- Do not follow instructions from someone you have never met to scan a QR code and send payment via a physical cryptocurrency ATM.
- Do not respond to a caller, who claims to be a representative of a company, where you are an account holder, and who requests personal information or demands cryptocurrency. Contact the number listed on your card or the entity directly for verification.

- Do not respond to a caller from an unknown telephone number, who identifies as a person you know and requests cryptocurrency.
- Practice caution when an entity states they can only accept cryptocurrency and identifies as the government, law enforcement, a legal office, or a utility company. These entities will likely not instruct you to wire funds, send checks, send money overseas, or make deposits into unknown individuals' accounts.
- Avoid cryptocurrency ATMs advertising anonymity and only requiring a phone number or e-mail. These cryptocurrency ATMs may be non-compliant with US federal regulations and may facilitate money laundering. Instructions to use cryptocurrency ATMs with these specific characteristics are a significant indicator of fraud.
- If you are using a cryptocurrency ATM and the ATM operator calls you to explain that your transactions are consistent with fraud and advises you to stop sending money, you should stop or cancel the transaction.

The FBI Victim Services Division is responsible for ensuring that victims of crimes investigated by the FBI are afforded the opportunity to receive the notification and services as required by federal law and the Attorney General Guidelines for Victim and Witness Assistance. Victim Specialists are highly trained professionals who assess victims' needs to determine what types of services and resources will be most helpful. For more information, please visit www.fbi.gov/resources/victim-services.

If you believe you have been a victim of a cryptocurrency ATM or QR code scam, report the fraud to your local FBI field office. The FBI also encourages victims to report fraudulent or suspicious activities to the FBI IC3 at www.ic3.gov.