THE NUMBERS:

Crypto ATMs are favored by criminals for their anonymity and general lack of oversight. Criminals rely on them as a fast, easy and often untraceable way to get access to victims' cash.

The Federal Reserve says crypto ATMs were used for at least $35 million in fraudulent transactions in 2022.

In 2023, consumer losses due to scams involving cryptocurrency ATMs, particularly Bitcoin ATMs, reached a concerning $114 million, a tenfold increase compared to $12 million in 2020.

During the first half of 2024, losses topped $65 million, with people 60 and older more than three times as likely as younger adults to report a loss.

Forest Lake had reported losses of nearly $300K in 2023 and 2024.

THE CRIME:

Impersonation: Pretending to be from a government agency (e.g., IRS, FBI), a well-known company (e.g., Apple, Microsoft), or even a family member in distress.

Threats: Threatening arrest, legal action, or account closure if the victim doesn't comply – missing jury duty.

Investment Scams: Promising high returns on cryptocurrency investments, often using fake websites or apps.

Romance Scams: Building a relationship online and then asking for money for fabricated emergencies.

Tech Support Scams: Claiming there's a problem with the victim's computer and requiring payment through a Bitcoin ATM to fix it.

THE VICTIMS:

Elderly and vulnerable population.

Retirees with established wealth.

Even if a victim is stopped during the scam and does not suffer a monetary loss, the mental and emotional impact is severe.

Some scams involve the impersonation of law enforcement, and the over-the-phone trust from actual law enforcement is lost.

THE INVESTIGATION:

Crypto currency fraud investigations take a considerable amount of time to investigate, not unlike any other high level financial crime.

The difference between a “normal” fiat currency financial crime and a virtual currency crime is the medium on which the crime occurs, which is a blockchain, and the level of cooperation you receive from the companies involved.

Tracing the path that the currency flows also takes expensive software.

THE LOOPHOLE:

Minnesota State Statute 53B.75 attempted to regulate the virtual currency kiosks to protect Minnesota residents.

Crypto currency kiosk companies determined a “loop hole” in the statute regarding the definition of a new customer.

Scammers will typically send a QR code to their victims that is linked to an established “wallet” or coin address, nullifying the entire section protecting new customers.

THE PREVENTION:

Education through presentations. AARP has been a tremendous resource and partner for the Forest Lake Police Department and has provided presentations to our community.

Self-regulation through a stricter business model by the kiosk companies.

Regulation through state statute or local ordinance.

THANK YOU

Nathan Olstad

Forest Lake Police Department

421@FLPD.COM

651-209-9926