# AG Consumer Protection

Bitcoin ATMs – Frequent Source of Scams and Money Laundering

Bitcoin ATMs have become a preferred tool for scammers looking to defraud unsuspecting victims—especially seniors. These transactions are not like traditional financial transactions. The money sent through Bitcoin ATMs is nearly impossible to recover. This fact makes them an attractive option for criminals engaged in fraud and money laundering.

## How Bitcoin ATM Scams Work

Scammers prey on the public's lack of familiarity with cryptocurrency. They exploit individual fears through sophisticated fraud schemes. A common scam targeting older adults involves a fraudulent message or phone call. The call might be from someone claiming to be with Apple, Google, or another well-known company, or even law enforcement. The scammer tells the victim that their financial accounts have been compromised. The call recipient is told they need to take immediate action to prevent unauthorized transactions on their account. If the scammer is pretending to be from a law enforcement agency, they may even threaten the victim with criminal prosecution or jail time if the victim doesn't pay a fine right away.

Victims are then instructed to withdraw large amounts of cash from their bank accounts. They are told to deposit the funds into a Bitcoin ATM. The cash is inserted and converted into Bitcoin. The victim is directed to scan and send a receipt or QR code to the scammer. The moment that transaction is completed, the money is gone — permanently. Traditional bank transfers, wire transfers, or credit card transactions have fraud prevention measures. These measures provide customer protection or financial institution safeguards to stop or reverse the transfer. That is not the case with Bitcoin ATM transactions.

## Why Bitcoin ATMs Are a Major Risk

Bitcoin ATMs lack oversight and regulation. For this reason, they are widely used for scamming and money laundering. Some consumers may attempt to use them for legitimate transactions. However, they often come with very high fees. The fees make them an inefficient and costly way to buy cryptocurrency. It's safer and cheaper to convert cash to cryptocurrency through a licensed and regulated online exchange.

Without regulation, victims of Bitcoin ATM scams have no meaningful consumer protections. They also have little or no recourse for recovering their stolen funds. Financial institutions have fraud prevention departments that monitor transactions. Banks can file suspicious activity reports (SARs) to investigate potential fraud. Unfortunately, Bitcoin ATMs operate outside these safeguards. They allow scammers to steal money quickly and anonymously.

## Real-Life Scams Cost Victims Thousands

Fraudsters employ Bitcoin ATMs for a well-known fraud scheme. They convince the victims that their Apple Pay or another account has been hacked. They urge the victim to withdraw their money and deposit it into a Bitcoin ATM. The scammers promise the money will be safe from hackers there in the ATM. The victim completes the transaction and sends a copy of the Bitcoin receipt to the scammers. The scammers then disappear with the money.

In another twist, the scammers may convince victims to download software onto their phones. This gives the criminals access to the victim's SIM card and phone data. The victims incur additional expenses when they discover they can only block the criminals' access to their information by purchasing another cell phone.

## A Call for Stronger Consumer Protections

Bitcoin ATMs are an unchecked risk for consumers. Michigan is not alone in facing this growing problem. Some states have taken action by limiting Bitcoin ATM transactions to $1,000 per day. The amount scammers can steal from victims in a single transaction is significantly reduced in this way. A similar limit in Michigan could have prevented an elderly couple from losing their entire life savings.

## How to Protect Yourself from Bitcoin ATM Scams

To avoid becoming a victim of a Bitcoin ATM scam, remember these key points:

- **No legitimate company or government agency will ever ask you to deposit money into a Bitcoin ATM**. If someone makes such a request, it's a scam
- **Beware of urgent requests**. Scammers create a sense of urgency to prevent victims from thinking critically about the request.
- **Do not trust caller ID**. Fraudsters can spoof phone numbers to make it appear as though they are calling from a trusted source
- **Never download unknown software or grant remote access to your devices**. This can allow scammers to take control of your personal information.
- **Talk to your bank before making large withdrawals**. If you're instructed to move money in an unusual way, seek advice first.
- **If you believe you have been targeted by a scam, report it immediately**. Scams can be reported to the Michigan Attorney General's Consumer Protection Team and local law enforcement.

Stay informed and help advocate for stronger regulations. In doing so, we can help protect consumers from the devastating impact of Bitcoin ATM scams. Urge your state legislators to support laws that limit these high-risk transactions if you are concerned about the lack of consumer protections surrounding Bitcoin ATMs.

## Contact the Attorney General's Office:

For general consumer questions or to file a complaint, you may reach the Michigan Department of Attorney General's Consumer Protection Team at:

Consumer Protection Team
P.O. Box 30213
Lansing, MI 48909
517-335-7599
Fax: 517-241-3771
Toll-free: 877-765-8388
Online complaint form

**Bitcoin ATMs – Frequent Source of Scams and Money Laundering**