

Bitcoin ATM Scams

Updated: Jan 2026



Bitcoin ATM scams are usually impersonation scams that push victims to withdraw cash and send it via a crypto kiosk/ATM using a QR code.

IC3 (2024): Complaints

10,956

Complaints involving crypto ATMs/kiosks

IC3 (2024): Losses

\$246.7M

Reported victim losses (crypto ATM/kiosk use)

Grand Forks area losses since 10/13/2022
(REPORTED)

\$466,803

Median reported loss

What stands out:

- IC3 reports crypto ATM/kiosk complaints rose 99% from 2023 → 2024.
- Losses cluster in tech support and impersonation narratives (government/business).
- Older adults are disproportionately harmed: FTC says 60+ reported ~71% of BTC ATM losses in 2024.
- Bitcoin ATMs charge 20–30% transaction fees

Cases REPORTED to GFPD since 10/13/2022


1	10/13/22	22107896	Vender Scam	\$8,500		Bitcoin ATM-Unknow-REMOVED
2	1/7/23	23100144	Bank Scam	\$8,400		Bitcoin Depot
3	3/17/23	23101662	Boss Scam	\$1,685		Bitcoin Depot
4	4/26/23	23102606	Tech Scam	\$9,100		Bitcoin Depot-REMOVED 6-7 months ago
5	7/19/23	23104818	Tech Scam	\$7,500		Bitcoin Depot-REMOVED 6-7 months ago
6	12/13/23	23108596	Tech scam	\$15,000		Bitcoin Depot-REMOVED 6-7 months ago
7	3/3/2024	24102188	Tech scam	\$27,900		Bitcoin Depot-REMOVED 6-7 months ago
8	2/3/25	23100749	Boss scam	\$12,600		Bitstop
9	3/20/25	25101787	Romance scam	\$150,000		Several locations
10	4/1/25	25102061	Warrant Scam	\$9,900		Bitcoin Depot
11	4/3/25	25102085	tech support	\$57,000.00		Bitcoin Depot
12	4/7/25	25102171	Boss scam	\$593		Bitcoin Depot
13	4/11/25	25102288	FTC LE scam	\$3,640		Coin Flip
14	4/22/25	25102561	warrant scam	\$6,300		Coin Flip
15	5/20/25	25103292	Tech Scam	\$12,500		Bitcoin Depot
16	6/16/25	25103942	Geeksquad	\$23,600.00		Bitcoin Depot
17	6/30/25	25104243	boss scam	\$1,800		Bitcoin Depot
18	7/7/25	EGFPD		\$25,000	sent from East Grand Forks	Bitcoin Depot
19	7/8/2025	IC3.gov	Tech Scam	\$15,000	Sent from East Grand Forks	Bitcoin Depot
20	7/14/25	IC3.gov	Sextortion	\$17,260.00		Coin Flip
21	7/16/25	22105397	Romance scam	\$5,000		Bitcoin Depot
22	7/28/25	25104926	Tech scam	\$14,700		Bitcoin Depot
23	7/29/25	25105029	Overpayment scam	\$12,300.00		Bitcoin Depot
24	7/31/25	25105057	warrant scam	\$10,500	Stopped by Police, was in process of sending \$15,000.00	Bitcoin Depot
25	8/4/25	25105151	warrant scam	\$3,900		Bitcoin Depot
26	11/14/25	22108737	Boss scam	\$725		Bitcoin Depot
27	11/21/2025	25108009	warrent scam	\$1,700		Bitcoin Depot
28	12/10/25	25108405	Warrant scam	\$2,700		Bitcoin Depot
29	12/29/25	25108747	Warrant Scam	\$2,000.00		Bitcoin Depot
30				\$466,803		

What is cryptocurrency and how does it work?

- A digital form of currency that exists only electronically on a Blockchain.
- Not issued or controlled by governments or banks.
- Uses cryptography to secure transactions.
- Users store their money in wallets (Coinbase wallet, Trust wallet) or exchanges (Coinbase, Binance, Crypto.com).
 - Only the user knows who owns their wallet, so long as it's not attached to an exchange.
 - Wallet and transactions are visible on the Blockchain.

Creating a new wallet address takes seconds

What a transaction looks like on the blockchain



bc1qz-enw69

USD

Bech32 (P2WPKH)

Bitcoin Address
bc1qz7c5fz3k0h7slfggdwaz4mm6z9eha533aenw69

Bitcoin Balance
0.00000000 • \$0.00






Wallet | Chart

Summary

This address has transacted 5 times on the Bitcoin blockchain. It has received a total of 0.20468714 BTC \$19,165.27 and has sent a total of 0.20468714 BTC \$19,165.27. The current value of this address is 0.00000000 BTC \$0.00.

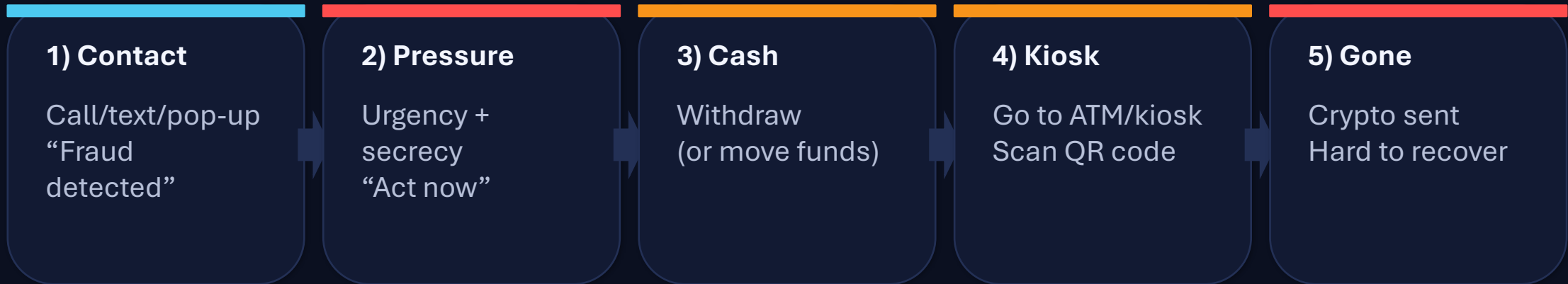
Total Received	0.20468714 BTC \$19,165.27	Total Sent	0.20468714 BTC \$19,165.27	Total Volume	0.40937428 BTC \$38,330.54
Transactions	5				

Transactions

	ID: 75d1-3743 7/30/2025, 13:23:42	From bc1q-nw69 To bc1q-ny0t	-0.02808481 BTC • -\$2,629.64 Fee 508 Sats • \$0.48	▼
	ID: bf54-cea0 7/30/2025, 13:20:38	From bc1q-nw69 To 2 Outputs	-0.02808367 BTC • -\$2,629.53 Fee 322 Sats • \$0.30	▼
	ID: a90a-c700 7/30/2025, 13:11:55	From bc1q-nw69 To 2 Outputs	-0.00213118 BTC • -\$199.55 Fee 605 Sats • \$0.57	▼
	ID: dca8-33ad 7/30/2025, 13:09:32	From bc1q-nw69 To 2 Outputs	-0.00383453 BTC • -\$359.03 Fee 322 Sats • \$0.30	▼
	ID: 0c58-c2b3 7/30/2025, 12:55:15	From bc1q-89pn To 34 Outputs	0.06213419 BTC • \$5,817.75 Fee 6.6K Sats • \$6.19	▼

Anatomy of a Bitcoin ATM scam

A typical flow (from first contact to irreversible transfer)



Key mechanic: QR code = destination wallet address

The scammer stays on the phone and gives step-by-step instructions until you scan a QR code at the kiosk. Once sent, the recipient controls the cryptocurrency and may move it immediately, making recovery difficult.

For Bitcoin Depot, the #1 Kiosk company used recently in Grand Forks for scams. You only need a phone number and PIN code to transfer money. No identification is required or asked for. This allows them to circumvent state law, which limits transactions of \$2000/day per customer.

Common scripts scammers use

Tech support / pop-up warnings

Fake “virus” or “Apple/Microsoft support” prompts
→ demands immediate payment via Bitcoin ATM.

Government or law enforcement impersonation

Claims you missed jury duty, have a warrant, owe fees, taxes, or your identity is tied to crimes
→ pay via kiosk to “resolve” or “secure” funds.

Business/bank impersonation

“Suspicious transaction” or “account compromised.”
→ withdraw cash and deposit at a Bitcoin ATM “for safety.”

Romance / lottery / extortion

Relationship building or threats
→ step-by-step kiosk instructions; QR code directs funds to a scammer.

IC3 2023: Tech support was the top kiosk-linked crime type (46% of complaints).

Bitcoin Kiosk companies in Grand Forks

4

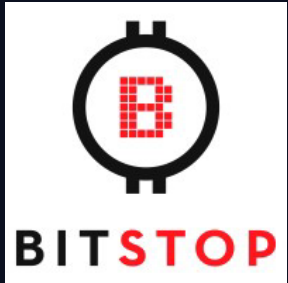


1



Stock photos

4



Friction & warnings on Bitcoin Depot ATM

WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:

- (1) Claims of a frozen bank account or credit card.
- (2) Fraudulent bank transactions.
- (3) Claims of identity theft or job offerings in exchange for payments.
- (4) Requests for payments to government agencies or companies.
- (5) Requests for disaster relief donations or loans.
- (6) Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.
- (7) Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.
- (8) Communication from someone impersonating a representative of your bank or a law enforcement officer.
- (9) IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.

b. WARNING: FUNDS LOST DUE TO USER ERROR OR FRAUD MAY NOT BE RECOVERABLE. TRANSACTIONS CONDUCTED ON THIS VIRTUAL - CURRENCY KIOSK ARE IRREVERSIBLE. I UNDERSTAND THESE RISKS AND WISH TO CONTINUE WITH CONDUCTING MY VIRTUAL - CURRENCY KIOSK TRANSACTION . PROTECT YOURSELF FROM FRAUD. NEVER SEND MONEY TO SOMEONE YOU DO NOT KNOW.

Friction & warnings on Bitcoin Depot Kiosk

Only required phone number and PIN to access a pre-made account.

WARNING: CONSUMER FRAUD OFTEN STARTS WITH CONTACT FROM A STRANGER WHO IS INITIATING A DISHONEST SCHEME. I UNDERSTAND THAT CRIMINAL ACTIVITY MAY APPEAR IN MANY FORMS, INCLUDING:

1. Claims of a frozen bank account or credit card.
2. Fraudulent bank transactions.
3. Claims of identity theft or job offerings in exchange for payments.
4. Requests for payments to government agencies or companies.
5. Requests for disaster relief donations or loans.
6. Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.
7. Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.
8. Communication from someone impersonating a representative of your bank or a law enforcement officer.
9. IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW

- exchange for payments.
4. Requests for payments to government agencies or companies.
 5. Requests for disaster relief donations or loans.
 6. Offers to purchase tickets for lotteries, sweepstakes, or drawings for vehicles.
 7. Prompts to click on desktop popups, such as virus warnings or communication from alleged familiar merchants.
 8. Communication from someone impersonating a representative of your bank or a law enforcement officer.
 9. IF YOU BELIEVE YOU ARE BEING SCAMMED, CALL A LOCAL LAW ENFORCEMENT OFFICER BEFORE ANY TRANSACTION.
 10. You may report fraudulent or criminal activity to your local police department and/or the North Dakota Attorney General.

Exit

Proceed

Enter your Mobile Number

Enter your mobile phone number to log in or sign up

+1 (000) 000-0000

1	2	3
4	5	6
7	8	9
+	0	X

Proceed

If someone else sent you to this machine and provided you with a QR Code or wallet ID to send funds to, it is most likely a scam.

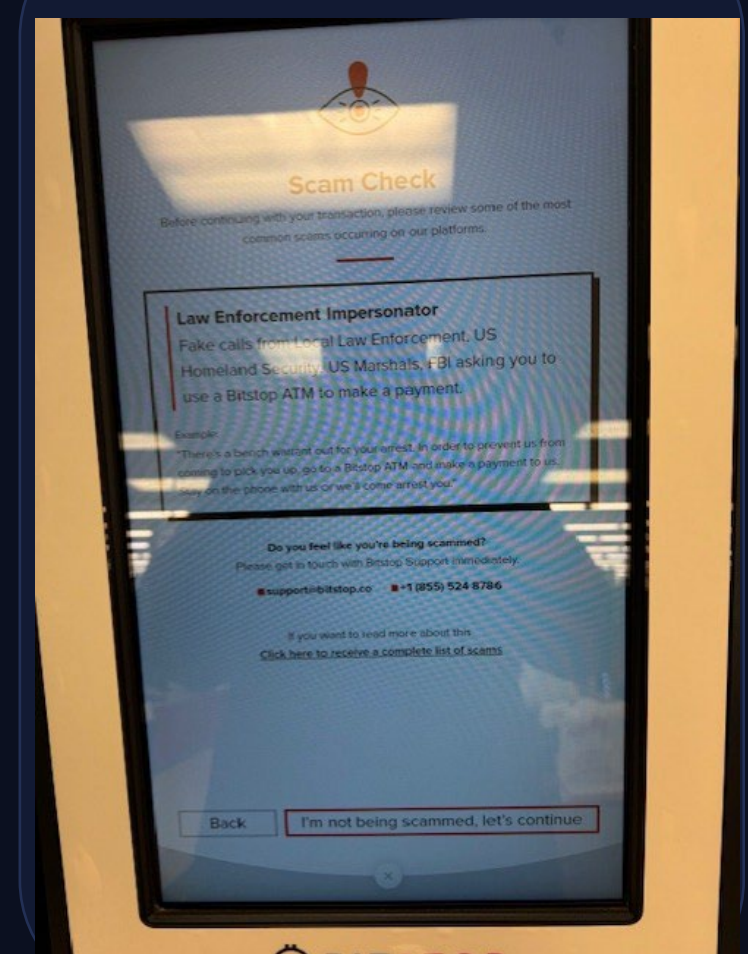
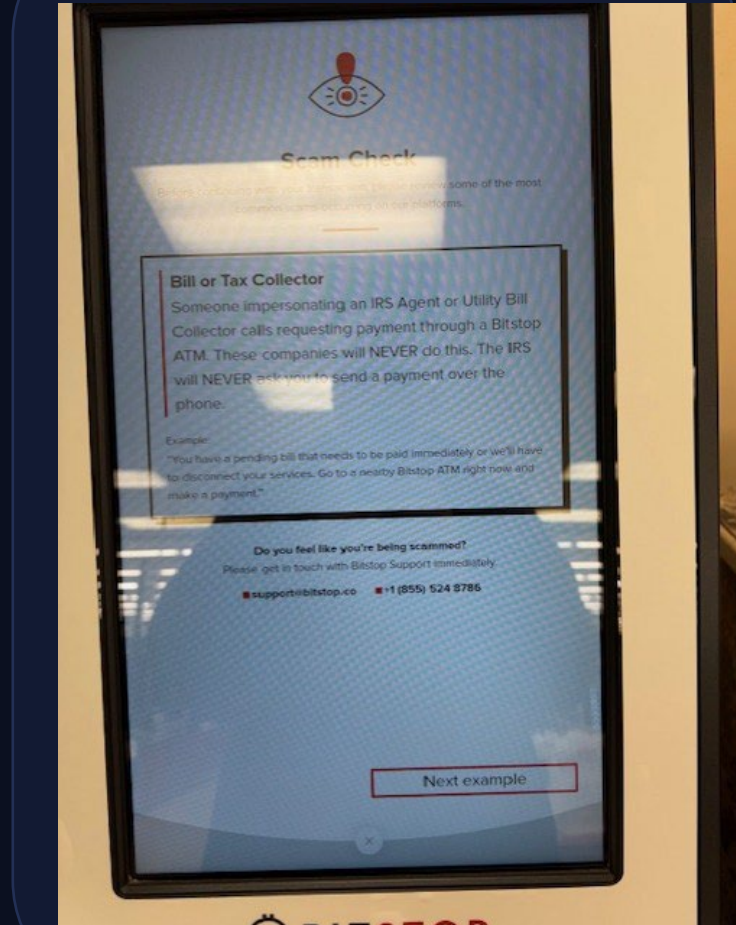
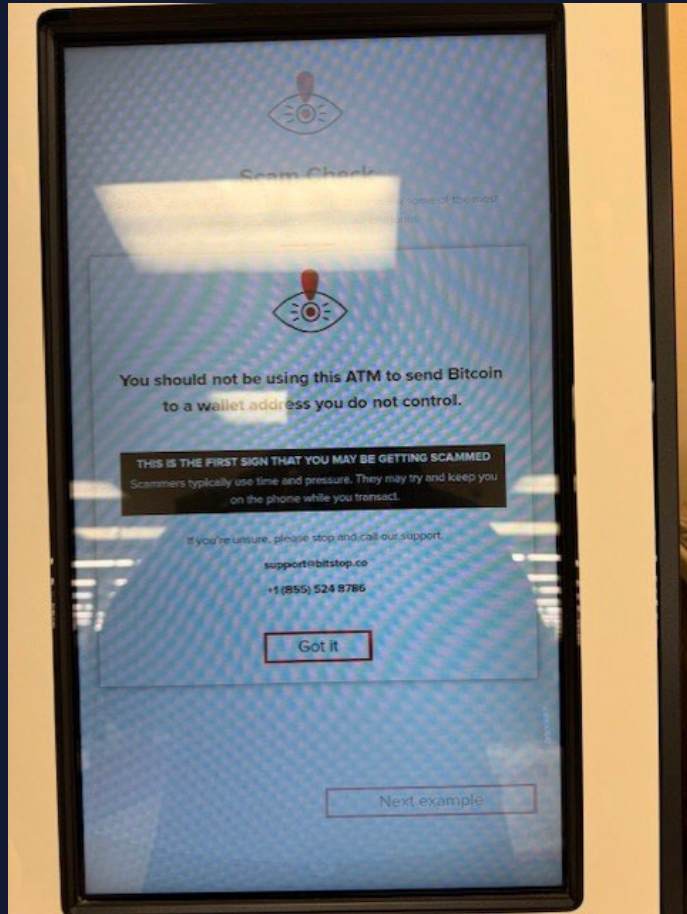
Friction & warnings on Coinflip Kiosk

Only required phone number and the original phone number are to access a pre-made account.



Friction & warnings on BitStop Kiosk

Only required phone number and PIN to access a pre-made account.



Daily Limits per customer

SECTION 5. Section 13-09.1-53 of the North Dakota Century Code is created and enacted as follows:

13 - 09.1 - 53 . Daily transaction limit.

A virtual - currency kiosk operator may not accept transactions of more than two thousand dollars of cash or the equivalent in virtual currency per calendar day with a single customer in this state via one or more virtual - currency kiosks operated by the same virtual-currency operator.

None of the kiosks ask for any form of identification when using a pre-existing account with a telephone number and PIN code, or a phone code.

Mitigations

Practical controls that could reduce harm

Friction & warnings

- Large, unavoidable scam warnings before purchase in large **RED** bold lettering requiring the user to “click” to acknowledge each warning.
- Confirmations: “Are you paying a stranger?” “Were you told to withdraw cash?” Again, in large **RED** bold lettering, requiring the user to click to acknowledge.
- Prominent signage near or on kiosks in high-risk locations.
- Businesses that house Bitcoin Kiosks must be educated in the signs of fraud.

Transaction safeguards recommendations

- User limits and daily caps, which require a valid state/gov’t identification for each transaction.
- The ability to cancel the transaction at any time, with full and immediate refund of the money inserted.
- Cooling-off delays for large cash-to-crypto purchases, meaning the money stays in an escrow account for 24-hours. Allowing the customer to cancel the transaction if they become aware that they were scammed.

Support, reporting & reimbursement

- Easy receipt details (kiosk address + wallet address) showing transaction cost prior to deposit and transaction.
- Full reimbursement to the customer for the first fraudulent transaction.
- Make a registry, so that it is know where each Bitcoin kiosk is.