ByteFederal

Securing the Bridge

Bitcoin ATMs, Financial Inclusion, and the Communities That Depend on Them

Prepared For:
Regulators, Policymakers & Community Stakeholders

Prepared By:
Byte Federal, Inc.
Venice, Florida

Date: March 2026
Version: 1.0

Contents

Executive Summary

At a Glance

Subject:	Bitcoin ATMs as critical financial infrastructure for underserved communities
Core Thesis:	Banning BTMs hurts 24.6M unbanked Americans while fraud migrates elsewhere
Key Data:	1.5% of internet crime losses; 98.8% legitimate; $26.6B check fraud vs $246.7M BTM
Solution:	Strengthen compliance at the kiosk; enforce upstream telecom rules
Audience:	Regulators, policymakers, and community stakeholders

Proposals to ban or severely restrict cryptocurrency kiosks — commonly known as Bitcoin ATMs (BTMs) — are gaining traction in state legislatures and regulatory agencies across the United States. These proposals are motivated by legitimate concerns about fraud targeting vulnerable populations, particularly the elderly. However, they rest on an incomplete understanding of both the fraud architecture and the communities that depend on these machines.

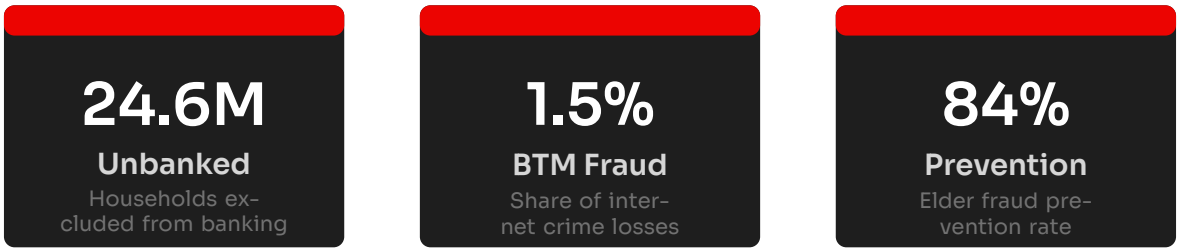
This policy brief presents the data that should inform — and constrain — that debate. It examines three questions:

1. **Who depends on Bitcoin ATMs?** The 24.6 million unbanked and underbanked American households for whom these kiosks are often the only regulated cash-to-digital conversion point.[1]
2. **How large is the fraud problem, in context?** Bitcoin ATM fraud represents 1.5% of total internet crime losses — a fraction of the losses from wire transfers, bank transfers, and check fraud.[2]
3. **What happens if you ban them?** Criminals redirect to other payment methods,

[1] Federal Deposit Insurance Corporation, 2023 National Survey of Unbanked and Underbanked Households (Oct. 2024).

[2] FBI Internet Crime Complaint Center (IC3), Internet Crime Report 2024 (reporting total losses of approximately $16.6 billion, of which $246.7 million involved convertible virtual currency kiosks).

while underserved communities lose a financial lifeline. The fraud migrates; the exclusion deepens.[3]



[3]FTC, Consumer Sentinel Network Data Book 2024 (Feb. 2025) (reporting that wire transfers, gift cards, and cash/mail collectively accounted for over $4 billion in fraud losses in 2024 — payment methods that would absorb redirected fraud volume if crypto kiosks were eliminated).

The Structural Architecture of Financial Exclusion

Who Is Excluded, Why, and What It Means for Policy

1.1 The Scale of the Problem

The magnitude of financial exclusion in the United States remains a profound socioeconomic challenge. According to the FDIC's 2023 National Survey — the authoritative benchmark for domestic financial inclusion data — approximately 4.2% of U.S. households, representing roughly 5.6 million discrete households, are entirely unbanked.[1] An additional 14.2% of households, representing 19.0 million house-

[1] FDIC, 2023 National Survey, supra note 1. In these households, no individual maintains a checking or savings account at a federally insured depository institution.

holds, are classified as underbanked.[2] Cumulatively, 18.4% of American households — roughly 24.6 million — remain structurally outside the mainstream financial ecosystem.

1.2 Who Is Excluded: The Demographics

The demographic composition reveals stark, persistent, and systemic inequities. Financial exclusion is highly correlated with race, income, educational attainment, and disability status.

Demographic	Unbanked Rate	Context
Native American households[3]	12.2%	6.4x the White household rate
Black households	10.6%	5.6x the White household rate
Hispanic households	9.5%	5.0x the White household rate
White households	1.9%	Baseline
Income under $15,000/yr	21.8%	1 in 5 households
No high school diploma	19.7%	25x the college graduate rate
Disability in household	11.2%	3x the national average
College graduates	0.8%	Baseline education level

KEY FINDING

Financial exclusion in America falls along lines of race, income, and disability. Any policy that removes financial infrastructure from underserved communities must be evaluated against its disparate impact on these populations.

1.3 Why People Are Unbanked: Systemic Barriers

The decision to remain unbanked is rarely a matter of consumer preference; it is the direct result of compounding structural barriers erected by the traditional banking industry.[4]

Minimum balance requirements. 42.3% of unbanked households cite the inability to meet minimum balance requirements as the single most significant reason for not maintaining an account.[5] The average minimum balance required to waive monthly maintenance fees on an interest-bearing checking account has reached a record $10,705.[6] For low-income consumers living paycheck to paycheck, sequestering this volume of idle capital is mathematically impossible.

Institutional distrust. 15.7% of unbanked households cite a deeply entrenched dis-

[2] FDIC, 2023 National Survey, supra note 1. Underbanked households technically possess a bank account but remain functionally marginalized, actively relying on nonbank alternative financial services.

[4] FDIC, 2023 National Survey, supra note 1. The survey asked unbanked households to identify their primary reasons for not having a bank account.

[5] Id.

[6] Bankrate, 2024 Checking Account and ATM Fee Survey (Jan. 2025).

trust of financial institutions as their primary deterrent.[7] This distrust is largely a behavioral response to punitive fee structures. In a recent year, financial institutions extracted over $7.7 billion in overdraft and non-sufficient funds (NSF) fees.[8] Alarmingly, 79% of these fees were borne by just 9% of account holders — a demographic predominantly composed of low-income, Black, and Hispanic consumers.[9] A standard $35 overdraft fee levied against a minor $26 overdraft, if repaid within three days, translates to an effective Annual Percentage Rate (APR) exceeding 16,000%.[10]

Administrative blacklisting. Over 80% of banks and credit unions utilize ChexSystems, a specialized consumer reporting agency that tracks banking infractions.[11] Often, these blanket denials are based on infractions as minor as a single bounced check or a briefly overdrawn balance, effectively imposing a multi-year exile from the formal banking sector.

Identification barriers. Approximately 13% of unbanked households cite a lack of personal identification as their primary barrier to entry.[12]

Physical geography. Between 2019 and 2023, the United States witnessed a 5.6% decline in physical bank locations, amounting to 5,413 branch closures.[13] As of mid-2024, 3,629 census tracts qualify as "banking deserts," leaving 12.3 million Americans without adequate branch access.[14] Majority-Black communities gained banking deserts at a rate of 10.1%, vastly outpacing the 6.4% national average.[15] Rural areas are now ten times more likely to be banking deserts than urban environments, with 40% of rural counties experiencing rapid branch loss.[16]

[7] FDIC, 2023 National Survey, supra note 1.
[8] Consumer Financial Protection Bureau, Data Point: Overdraft/NSF Fee Reliance Since 2015 (2024).
[9] Id.
[10] Center for Responsible Lending, Overdraft Fees: Banks Must Stop Gouging Consumers During Economic Crisis (2024).
[11] ChexSystems, Inc., About Us: Consumer Assistance (2025). ChexSystems maintains derogatory records for up to five years and facilitates the denial of accounts to over one million people annually.
[12] FDIC, 2023 National Survey, supra note 1.
[13] National Community Reinvestment Coalition, Bank Branch Closures and Banking Deserts: 2023 Update (2024).
[14] Id.
[15] Id.
[16] Id.

The Cash-to-Digital Bridge

What Bitcoin ATMs Do, Who Uses Them, and Why They Matter

2.1 What Bitcoin ATMs Actually Do

Bitcoin ATMs and digital asset transaction kiosks are physical, unattended or semi-attended terminals that allow customers to insert fiat currency (paper banknotes) in exchange for equivalent values of cryptocurrency, or conversely, to sell cryptocurrency for dispensed physical cash.[1]

Unlike online cryptocurrency exchanges such as Coinbase or Kraken — which offer significantly lower trading fees but mandate that users link a traditional bank

[1] Financial Crimes Enforcement Network (FinCEN), Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013) (classifying operators of cryptocurrency kiosks as money transmitters under the Bank Secrecy Act).

account or debit card to fund their digital wallets — BTMs bypass the legacy financial system entirely.[2] They act as the only mainstream, regulated, physical cash-to-digital conversion point that requires no pre-existing bank account, directly addressing the core barriers that keep the unbanked excluded.

2.2 Who Uses Them

Behavioral data indicates that these kiosks are not primarily utilized by sophisticated cryptocurrency traders, but rather by everyday consumers seeking a gateway into digital finance. A survey conducted by CoinFlip, the second-largest U.S. operator, revealed that 74% of their users made their first-ever cryptocurrency transaction at a physical kiosk.[3]

A critical segmentation insight is that the "unbanked" demographic is not a homogeneous entity. A substantial portion is "cash-only," meaning they utilize neither prepaid debit cards nor nonbank payment applications.[4] Cash-only households are disproportionately older, more likely to be Hispanic, and highly likely to cite a deep distrust of banks as their primary reason for remaining unbanked.[5] For this specific sub-segment, the physical kiosk serves as an indispensable tool.

The primary motivations for utilizing these kiosks cluster around four core consumer needs: **conversion** (physical cash into digital value), **obligations** (paying utility bills and rent through integrated bill-pay networks), **access** (24-hour availability in retail environments vs. limited bank branch hours), and **control** (tangible printed receipts, physical confirmation, and strict "cash budgeting" without the risk of automated, unexpected overdraft fees).[6]

2.3 The Remittance Use Case

Perhaps the most compelling financial inclusion argument centers on cross-border remittances. Immigrant populations, unbanked laborers, and migrant workers frequently send vital portions of their income to families abroad. Traditional remittance channels are notoriously slow, technologically archaic, and highly extractive. According to early 2025 data from the World Bank, global average remittance costs stand at 6.49% for a standard $200 transfer, with traditional banking institutions charging a staggering global average of 14.55%.[7]

Cryptocurrency architecture fundamentally disrupts this extractive model. Transfers executed using fiat-pegged stablecoins on low-cost blockchain networks in-

[2] See, e.g., Coinbase, Terms of Service (2025) (requiring linked bank account or debit card for fiat-funded transactions); Kraken, Funding Methods (2025) (same).

[3] CoinFlip, 2024 Consumer Survey: Understanding Bitcoin ATM Users (2024). CoinFlip operates approximately 5,500 machines processing over $4 billion in cumulative volume.

[4] FDIC, 2023 National Survey, supra note 1 (reporting that 66.2% of unbanked households use only cash for day-to-day transactions).

[5] FDIC, 2023 National Survey, supra note 1 (demographic analysis of cash-only unbanked households).

[6] Pew Research Center, How Americans Use Cash (2024); FDIC, 2023 National Survey, supra note 1 (identifying access, cost, trust, and control as the four primary factors influencing financial service selection among unbanked populations).

[7] World Bank, Remittance Prices Worldwide Quarterly Report (Q1 2025). In critical U.S. outbound corridors — such as Mexico ($64.7 billion received in 2024) or the Philippines ($12.8 billion) — traditional money transfer operators routinely charge between 5% and 8%.

cur network routing fees ranging from mere pennies to $5 per transaction, regardless of the principal amount transferred.[8] The decentralized finance (DeFi) Education Fund estimates that crypto and DeFi infrastructure could reduce total global remittance costs by up to 80%, potentially saving $30 billion annually worldwide.[9] For a migrant worker sending $500 monthly, even a partial fee reduction could return over $300 per year — equivalent to nearly a month's worth of transfers.[10]

[8] See, e.g., Stellar Development Foundation, Stellar Network Fee Structure (2025) (base fee of 0.00001 XLM, approximately $0.000001 at current prices); Tron Foundation, USDT-TRC20 Transaction Costs (2025) (typical fees of $1–$3 per transfer).

[9] DeFi Education Fund, The Case for DeFi: Financial Inclusion Through Decentralized Infrastructure (2024).

[10] Calculation based on World Bank average remittance cost of 6.49% ($32.45 per $500 transfer) vs. crypto network fees of approximately $2 per transfer, yielding savings of approximately $30.45/month or $365/year.

Fraud in Context

What the Data Actually Shows

3.1 The Scale of BTM Fraud

The fraud concerns motivating regulatory action are real but must be understood in proportion. The FBI's Internet Crime Complaint Center reported that in 2024, it received 10,956 formal complaints involving convertible virtual currency kiosks, culminating in approximately $246.7 million in reported victim losses.[1] This represented a 99% increase in complaint volume and a 31% increase in financial losses from the previous year.[2]

The human cost is concentrated among the elderly. FTC data reveals that consumers

[1] FBI IC3, Internet Crime Report 2024, supra note 2.
[2] Id.

over the age of 60 are more than three times as likely to report losing money via a BTM scam.[3] Older adults account for over 71% of all reported Bitcoin ATM scam losses.[4]

These numbers are concerning. They are also a small fraction of the overall fraud landscape.

3.2 Fraud by Payment Method

Payment Method	Fraud Losses	Share of Total
Check Fraud (Global)[5]	$26.6B	—
Bank Transfers / BEC[6]	$2.09B	12.6%
Gift Cards[7]	$1.03B	6.2%
Wire Transfers[8]	$287M	1.7%
Bitcoin ATMs[9]	$246.7M	1.5%

KEY FINDING

Bitcoin ATM fraud represents **1.5% of total internet crime losses**. Wire transfers alone account for more fraud. Bank transfer fraud is **8.5 times larger**. Yet no one is proposing to ban wire transfers or shut down banks.

3.3 The Legitimate Transaction Rate

Industry-wide data from Chainalysis shows that **98.8% of all BTM transactions are legitimate**.[10] The illicit transaction rate of 1.2% is comparable to or below the rates observed in other financial sectors.[11]

[3] FTC, Consumer Sentinel Network Data Book 2024, supra note 3.

[4] Id.

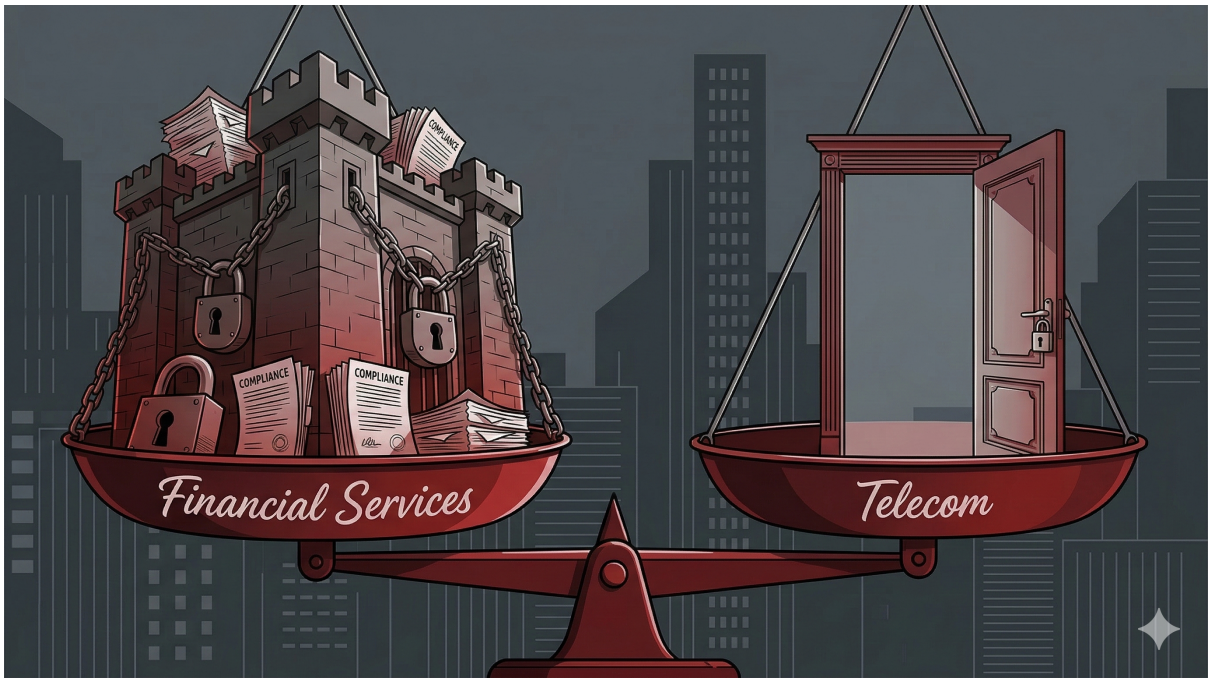
[10] Chainalysis, 2024 Crypto Crime Report (2024). Illicit activity accounted for approximately 1.2% of total BTM transaction volume, consistent with or below the illicit transaction rate for the broader cryptocurrency ecosystem.

[11] See United Nations Office on Drugs and Crime, Money-Laundering and Globalization (estimating that 2–5% of global GDP, or $800 billion to $2 trillion, is laundered annually through the traditional banking system). The BTM illicit rate of 1.2% is substantially below this range.

4

What Happens When You Ban the Bridge

Fraud Migrates, Communities Lose



4.1 Fraud Migrates, It Doesn't Disappear

Banning Bitcoin ATMs would not eliminate the upstream fraud infrastructure. The scam call still originates from a VoIP provider with ineffective identity screening.[1] The spoofed caller ID still reaches the victim. The social engineering still works. The victim still goes to the bank and withdraws cash.

The only thing that changes is the final payment method. Instead of a Bitcoin ATM, the victim is directed to:[2]

[1] See Byte Federal, Inc., The Architecture of Exploitation: How Scammers Exploit the Telecom Regulatory Gap (Mar. 2026) (detailing the five-stage scam architecture in which the crypto ATM is Stage 5 — the final endpoint after origination, transmission, social engineering, and bank withdrawal).

[2] FTC, Consumer Sentinel Network Data Book 2024, supra note 3 (reporting fraud losses by pay-

- **Wire transfers** — $287 million in fraud losses (2024)
- **Gift cards** — $1.03 billion in fraud losses (2024)
- **Cash by mail** — untraceable, unrecoverable
- **Peer-to-peer payment apps** — minimal fraud prevention compared to regulated BTMs

None of these alternatives offers the compliance infrastructure that a regulated Bitcoin ATM operator provides: mandatory KYC, SAR filing, AI-powered behavioral detection, or live human intervention.

4.2 The Communities That Lose

If Bitcoin ATMs are banned, the 24.6 million unbanked and underbanked Americans described in Chapter 1 lose access to:

- The only regulated cash-to-digital conversion point available without a bank account
- A remittance channel that can reduce transfer costs by up to 80%[3]
- 24-hour access to financial services in retail locations (vs. limited bank branch hours)
- Entry into the digital economy — without which they cannot participate in e-commerce, digital bill payment, or digital savings

THE DISPARATE IMPACT

A Bitcoin ATM ban falls heaviest on Native American households (12.2% unbanked), Black households (10.6%), Hispanic households (9.5%), households earning under $15,000 (21.8%), and households without a high school diploma (19.7%). These are the same communities that the banking system has already failed.[a]

[a] FDIC, 2023 National Survey, supra note 1. See also National Community Reinvestment Coalition, supra note 19 (documenting that bank branch closures disproportionately affect majority-Black and rural communities).

ment method, demonstrating that scammers routinely adapt to use whichever payment channel is available).

[3] DeFi Education Fund, supra note 29.

5

The Alternative Financial Services Comparison

What the Unbanked Actually Pay Today

Critics of Bitcoin ATM fees — which typically range from 10% to 25% of the transaction value[1] — often compare them unfavorably to online exchange fees of 0.5–1%. This comparison is analytically flawed. For the 24.6 million unbanked and underbanked households, online exchanges that mandate linked checking accounts are completely inaccessible.[2] The relevant comparison is not to Coinbase but to the alternative financial services these populations are forced to use:

Service	Typical Cost	Annual Cost (Frequent User)
Bitcoin ATM	10–25% per transaction[3]	Variable by volume
Check Cashing	1.5–5.0% of check value[4]	$1,000–$1,200/yr
Payday Loans	$15/$100 (391% APR)[5]	$400–$800+/yr
Bank Overdraft/NSF	$27–$35 per event (>16,000% APR)[6]	$380+/yr
Prepaid Debit Cards	Monthly + reload + ATM fees[7]	$200–$300/yr
Money Orders	$1.75–$10.00 each[8]	$24–$120/yr
Remittance (Western Union)	5–8% per transfer[9]	$300–$600/yr

While a 15% BTM fee is extractive on a per-transaction basis, it is a one-time transactional cost. It does not create debt spirals, recurring monthly charges, or compound fees. Compare this to payday loans bearing a 391% APR, which drained over

[1] Industry averages compiled from operator fee disclosures. Lower-cost operators like CoinFlip average around 7.1% plus a flat fee; the overall industry average remains in the 10–25% range including exchange rate spreads.

[2] FDIC, 2023 National Survey, supra note 1.

$2.4 billion in fees from low-income borrowers in a single year.[10]

Furthermore, Bitcoin ATMs convert physical cash into a borderless digital asset that unlocks an entire ecosystem of decentralized financial services — savings, lending, cross-border transfers — that no other alternative financial service can provide.[11]

[10] CFPB, Payday Lending: Final Rule, supra note 44.

[11] See DeFi Education Fund, supra note 29 (estimating that DeFi infrastructure could save underserved populations $30 billion annually in financial service costs).

6

The Regulatory Framework That Already Exists

BTM Operators Are Among the Most Regulated Financial Entities

Bitcoin ATM operators are not operating in a regulatory vacuum. They are among the most heavily regulated financial entities in the United States:

- **FinCEN Registration:** Mandatory federal registration as Money Services Businesses under 31 U.S.C. § 5330.[1]
- **AML Program:** Mandatory 5-pillar anti-money laundering program under 31 C.F.R. § 1022.210, including internal controls, compliance officer designation, employee training, independent review, and risk assessment.[2]
- **Suspicious Activity Reports:** Mandatory SAR filing for transactions of $2,000 or more that are suspicious — a lower threshold than the $5,000 required for banks.[3]
- **Currency Transaction Reports:** Mandatory CTR filing for transactions over $10,000.[4]
- **State Money Transmitter Licenses:** Required in approximately 48 states, with varying surety bond requirements often reaching millions of dollars.[5]
- **OFAC Compliance:** Mandatory screening against the Office of Foreign Assets Control's Specially Designated Nationals list.[6]
- **Criminal Penalties:** Operating an unlicensed money transmitting business is a federal felony punishable by up to 5 years imprisonment.[7]

[1] 31 U.S.C. § 5330; 31 C.F.R. § 1022.380.
[2] 31 C.F.R. § 1022.210.
[3] 31 C.F.R. § 1022.320(a)(2) (MSB threshold) vs. 31 C.F.R. § 1020.320 (bank threshold).
[4] 31 C.F.R. § 1010.311; 31 U.S.C. § 5313.
[5] See, e.g., Fla. Stat. § 560.103; N.Y. Banking Law § 641.
[6] 31 C.F.R. Part 501.
[7] 18 U.S.C. § 1960.

Annual compliance costs for a major BTM operator range from $500,000 to over $2 million.[8] By contrast, a VoIP telecom provider — the entity that actually initiates the fraud — can begin operating with a $100 filing fee and no meaningful compliance infrastructure.[9]

[8] Industry estimates based on public filings and operator disclosures. Costs include licensing fees, surety bonds, compliance staff, legal counsel, technology infrastructure, SAR/CTR filing systems, and independent audit requirements.

[9] 47 C.F.R. § 64.6305; see Byte Federal, The Architecture of Exploitation, supra note 38.

7

Byte Federal's Approach: Protecting the Bridge

Industry-Leading, Multi-Layered Fraud Prevention

Rather than waiting for regulatory mandates, Byte Federal has built an industry-leading, multi-layered fraud prevention system:[1]

1. **Banking-grade KYC:** Government-issued ID verification, selfie-to-ID biometric matching, SSN verification, and OFAC screening for all customers — exceeding the Customer Identification Program requirements applicable to banks.[2]
2. **AI-powered behavioral detection:** Camera-based analysis detects coercion signals (urgent bill-feeding, phone script-reading, visible distress), with automatic transaction halt capability.
3. **Mandatory scam education:** 30-second warning screens with randomized button placement, explicit scam scenario warnings, and multiple automated text messages post-registration.[3]
4. **Live human intervention:** For every customer over 60 identified as a potential scam victim, a trained compliance team member calls the customer directly, in real time — achieving an **84% prevention rate**.[4]
5. **Anti-fraud Terms of Service:** Explicit prohibition on third-party-directed transactions; permanent platform ban for users who transact to wallets that are not their own.[5]

Byte Federal spearheaded a revision to the Florida Money Transmitter Laws signed in June 2022, and was subsequently asked by the Florida Office of Financial Reg-

[1] Byte Federal, Inc., Scam Deterrents, Counter Measures, and Due Diligence, Letter to the Florida Office of Financial Regulation (July 11, 2024).
[2] 31 C.F.R. § 1020.220 (bank CIP requirements). Byte Federal's process includes additional biometric and behavioral verification layers.
[3] Byte Federal, Scam Deterrents, supra note 60.
[4] Byte Federal, Inc., internal compliance data (2024–2025).
[5] Byte Federal, Scam Deterrents, supra note 60.

ulation to help create policies and procedures for the entire virtual currency kiosk industry.[6]

[6] Byte Federal, Scam Deterrents, supra note 60.

Conclusion: Protect Consumers by Protecting the Bridge

The Policy Choice Before Us

The policy choice is not between "protecting consumers" and "preserving Bitcoin ATMs." The real choice is between:

1. **Banning the endpoint** — eliminating a regulated, monitored financial service that serves 24.6 million unbanked and underbanked Americans, while criminals redirect to less-regulated payment methods. Fraud migrates; financial exclusion deepens.
2. **Securing the bridge** — strengthening compliance at the kiosk level (as Byte Federal has done), while simultaneously addressing the upstream causes of fraud: ineffective telecom KYC, unenforced caller ID spoofing laws, and the absence of

Confirmation of Payee at the bank level.

THE PATH FORWARD

1. **Enforce existing telecom laws:** The FCC's rules already require providers to "know their customers"[a] — enforce them with the same rigor applied to financial institutions.
2. **Mandate industry-wide BTM fraud prevention standards:** Require all operators to implement the multi-layered protections Byte Federal has built voluntarily.
3. **Adopt Confirmation of Payee at the bank level:** A proven 50% fraud reduction measure, already mandated in the UK.[b]
4. **Protect the bridge:** Do not ban the only regulated cash-to-digital conversion point available to America's most financially excluded communities.

[a] 47 C.F.R. § 64.6305(b).
[b] UK Payment Systems Regulator, Confirmation of Payee: Implementation and Impact Assessment (2024).

THE BOTTOM LINE

Banning Bitcoin ATMs addresses 1.5% of internet crime losses while removing financial infrastructure from communities that are already excluded from the banking system. Enforce existing laws upstream. Strengthen compliance at the kiosk. Protect the bridge that serves 24 million Americans.

Prepared by: Byte Federal, Inc. | March 2026 | bytefederal.com/fraud-prevention

Companion documents: The Architecture of Exploitation (fraud architecture analysis) | Closing the Telecom Regulatory Gap (telecom regulatory deep dive)

Bibliography

Consolidated Reference List — All Sources Cited in This Report

This bibliography compiles all sources cited in the footnotes of this report into a single, independently printable reference list. Sources are organized by category for ease of navigation.

A.1 Federal Statutes & Regulations

[1] 18 U.S.C. § 1960 (Unlicensed Money Transmitting Business)

[2] 31 U.S.C. § 5313 (Reports on Domestic Coins and Currency Transactions)

[3] 31 U.S.C. § 5330 (Registration of Money Transmitting Businesses)

[4] 47 C.F.R. § 64.6305 (Robocall Mitigation Database Requirements)

[5] 31 C.F.R. § 1010.311 (Currency Transaction Report Requirements)

[6] 31 C.F.R. § 1020.220 (Customer Identification Program — Banks)

[7] 31 C.F.R. § 1020.320 (Suspicious Activity Report — Banks)

[8] 31 C.F.R. § 1022.210 (Anti-Money Laundering Program — MSBs)

[9] 31 C.F.R. § 1022.320 (Suspicious Activity Report — MSBs)

[10] 31 C.F.R. § 1022.380 (MSB Registration Requirements)

[11] 31 C.F.R. Part 501 (OFAC Regulations)

[12] Fla. Stat. § 560.103 (Florida Money Services Business Act)

[13] N.Y. Banking Law § 641 (Money Transmitter Licensing)

A.2 Government Reports & Data

[14] Federal Deposit Insurance Corporation, 2023 National Survey of Unbanked and Underbanked Households (Oct. 2024)

[15] Federal Trade Commission, Consumer Sentinel Network Data Book 2024 (Feb. 2025)

[16] FBI Internet Crime Complaint Center, Internet Crime Report 2024

[17] FBI IC3, 2024 Elder Fraud Report (2025)

[18] FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013)

[19] United Nations Office on Drugs and Crime, Money-Laundering and Globalization (global estimates)

[20] UK Payment Systems Regulator, Confirmation of Payee: Implementation and Impact Assessment (2024)

A.3 Industry Research & Consumer Data

[21] Chainalysis, 2024 Crypto Crime Report (2024)

[22] CoinFlip, 2024 Consumer Survey: Understanding Bitcoin ATM Users (2024)

[23] National Community Reinvestment Coalition, Bank Branch Closures and Banking Deserts: 2023 Update (2024)

[24] Bankrate, 2024 Checking Account and ATM Fee Survey (Jan. 2025)

[25] Consumer Financial Protection Bureau, Data Point: Overdraft/NSF Fee Reliance Since 2015 (2024)

[26] CFPB, Payday Lending: Final Rule (2024)

[27] Center for Responsible Lending, Overdraft Fees: Banks Must Stop Gouging Consumers During Economic Crisis (2024)

[28] ChexSystems, Inc., About Us: Consumer Assistance (2025)

[29] Pew Research Center, How Americans Use Cash (2024)

[30] Pew Charitable Trusts, Why Americans Use Prepaid Cards (2024)

[31] American Bankers Association, Global Check Fraud Report (2024)

[32] World Bank, Remittance Prices Worldwide Quarterly Report (Q1 2025)

[33] DeFi Education Fund, The Case for DeFi: Financial Inclusion Through Decentralized Infrastructure (2024)

[34] Stellar Development Foundation, Stellar Network Fee Structure (2025)

[35] Tron Foundation, USDT-TRC20 Transaction Costs (2025)

[36] U.S. Postal Service, Money Order Pricing (2025)

[37] Western Union, Fee Schedule (2025)

A.4 Byte Federal Sources

[38] Byte Federal, Inc., Scam Deterrents, Counter Measures, and Due Diligence, Letter to the Florida Office of Financial Regulation (July 11, 2024)

[39] Byte Federal, Inc., Internal Compliance Data: Elder Fraud Prevention Outcomes (2024–2025)

[40] Byte Federal, Inc., The Architecture of Exploitation: How Scammers Exploit the Telecom Regulatory Gap (Mar. 2026)