ByteFederal

THE ARCHITECTURE OF EXPLOITATION

How Scammers Exploit the Telecom Regulatory Gap
— and How Byte Federal Stops Them

A Data-Driven Briefing

Fraud Architecture | Regulatory Failure | Industry-Leading Prevention

$12.5 Billion in Annual Fraud Losses
52.5 Billion Robocalls in 2025
84% Elder Fraud Prevention Rate

Prepared by:
Byte Federal, Inc.

March 2026

This document is intended for regulators, policymakers, law enforcement, and press. Distribution is encouraged.

Contents

1 The Scale of the Crisis

Despite years of promises, the fraud epidemic targeting American consumers — particularly seniors — has not improved. The data for 2024–2025 paints a stark picture of systemic failure.

Robocalls received by Americans in 2025 — the highest volume since 2019.
Source: YouMail Robocall Index

$12.5B	**+43%**	**$4.9B**
Total Fraud Losses (2024)	Elder Fraud Surge (YoY)	Reported Elder Losses

IMPORTANT

FBI elder fraud figures are dramatically undercounted. Victims often feel shame and do not report losses to family members or law enforcement. The true figure is estimated to be exponentially higher than the $4.9B reported.

Phone calls remain the **primary fraud vector**, producing the highest median individual loss of any contact method:

Contact Method	Median Loss per Victim	Risk Level
Phone Call	$2,210	**CRITICAL**
Social Media	$580	High
Email	$120	Moderate

2 The Scam Architecture: A Step-by-Step Chain of Custody

The modern elder fraud scam is a highly engineered process that exploits gaps in two major regulatory systems — telecommunications and banking — before arriving at a financial endpoint. Understanding each stage is critical to understanding where the system fails.

We strictly regulate the **EXIT door** (banks, crypto ATMs) but leave the **FRONT DOOR** (telecom) completely unlocked. The crime is initiated in telecom; the money is lost in finance.

2.1 Stage 1 — Origination: The Unlocked Front Door

The scam begins when a bad actor purchases access to the US telephone grid through a Voice over IP (VoIP) provider. Prior to 2025, this required virtually no verification:

- $100 filing fee to the FCC Robocall Mitigation Database (RMD) — the only barrier to entry
- No background checks, no surety bonds, no suspicious activity reports
- No identity verification — fictional names, hotel addresses, and anonymous cryptocurrency payments were accepted as standard practice

A bad actor registered with VoIP provider Telnyx LLC under the alias "MarioCop," listing a Sheraton Hotel in Canada as his corporate address and paying with anonymous Bitcoin via a throwaway email address. He was approved and subsequently originated hundreds of government imposter scam calls.

"In banking, this onboarding would be a federal crime. In telecom, it was standard practice until 2025."

In 2025, the FCC issued its first-ever Know Your Customer (KYC) enforcement action against a VoIP provider — a $4.5M proposed fine against Telnyx — marking a historic but belated recognition of the problem.

2.2 Stage 2 — Transmission: The Call Travels Undetected

Once originated, the fraudulent call travels through intermediate carriers. The $250 million STIR/SHAKEN caller ID authentication technology, meant to prevent spoofing, fails at this stage through two critical engineering gaps:

Failure #1: The Legacy TDM Bypass	**Failure #2: The A-Level Trust Paradox**
STIR/SHAKEN travels with calls as a digital watermark. When a call is routed through legacy copper wire (TDM) networks — still common in rural America — the digital signature is stripped entirely. Scammers deliberately route traffic through rural exchanges to "wash" their calls.	Providers grant scammers the highest possible trust rating (A-Level attestation) based purely on having a billing relationship — without inspecting call content. In the 2024 New Hampshire primary deepfake incident, Lingo Telecom stamped A-Level trust on an AI-generated call impersonating the president telling voters not to vote.

The FCC has historically collected less than **0.003%** of issued fines — only $6,790 of $208 million levied since 2015. Penalties are functionally non-existent, making fines a negligible cost of doing business.

2.3 Stage 3 — The Hook: Social Engineering via Spoofed Identity

The scam call reaches the victim with a spoofed caller ID displaying a trusted number — a government agency, Social Security Administration, IRS, Medicare, bank fraud department, or tech support. The scammer uses high-pressure social engineering tactics:

- Creates false urgency — arrest warrants, account compromise, IRS debt, computer virus
- Instructs the victim to keep the call confidential — isolating them from family intervention
- Directs the victim to immediately withdraw cash or make a payment
- Maintains live phone presence throughout the entire transaction to prevent second-guessing

41% of high-loss senior scams originate with a phone call, which produces the highest median individual losses of any fraud vector at $2,210 per incident.

2.4 Stage 4 — The Bank: A Monitor Without a Guardian

The victim proceeds to their bank to withdraw cash, often thousands of dollars. Banks represent a critical but largely missed intervention point:

What Banks Are Required to Do	What Banks Are Not Required to Do
File CTRs for cash withdrawals over $10,000	Deny access to funds based on suspected fraud
File SARs for transactions over $5,000	Proactively warn customers about scam patterns
Maintain transaction logs for regulatory review	Verify wire transfer recipient identity (no Confirmation of Payee mandate in US)
KYC identity verification at account opening	Halt a transaction because a senior is on their phone reading a script

BOTTOM LINE

Banks are legally deputized as **MONITORS**, not **GUARDIANS**. They document the crime — they are not required to stop it. Federal law does not explicitly mandate denial of access to funds even when fraud is suspected.

The UK's Confirmation of Payee (CoP) system — which verifies that the account name matches the intended recipient before processing a wire — **reduced fraud by 50%** after mandated implementation. The US has not adopted a comparable requirement as of 2026.

In 2024, bank wire fraud resulted in $2.09 billion in losses — nearly **nine times** the fraud attributed to Bitcoin ATMs, yet the bank channel receives far less regulatory scrutiny.

2.5 Stage 5 — The Crypto ATM: The Heavily Regulated Final Endpoint

After withdrawing cash, the victim is directed to a Bitcoin ATM (BTM) to complete the payment. Contrary to widespread misconception, BTM operators are among the most heavily regulated financial entities in the United States:

Bitcoin ATM Operators	VoIP Telecom Providers
AML Program — **Mandatory** 5-Pillar Framework	AML Program — **NONE**
SARs — **Mandatory** for transactions over $2,000	SARs — **NONE**
State Money Transmitter Licenses — **Required in ~48 states**	State Licensing — Federal FCC only ($100 fee)
FinCEN Registration — **Mandatory** Federal	FinCEN Registration — **NOT REQUIRED**
Surety Bonds — **Millions required** to operate	Surety Bonds — **NONE**
Operating without license: **Federal Felony**	Operating without registration: Minor fine (often uncollected)
Annual Compliance Cost: **$500K – $2M+**	Annual Compliance Cost: ~$100 filing fee

Crypto kiosk operators spend **5,000 times more** on compliance annually than VoIP providers. The fraud begins in the most lightly regulated industry and ends in one of the most heavily regulated.

Industry-wide data shows that **98.8% of all BTM transactions are legitimate**. Illicit

activity accounts for only 1.2%.

3 The Regulatory Asymmetry: Why the System Is Upside Down

The core structural problem enabling elder fraud is not criminal sophistication — it is a profound mismatch in regulatory burden between the industry that initiates fraud and the industry that terminates transactions.

> We have built a financial fortress around the exit points for money (banks, crypto ATMs) while leaving the entry point for fraud — the phone network — operating as the wild west.

3.1 The STIR/SHAKEN Technology Failure

- $250 million invested in STIR/SHAKEN caller authentication technology
- Only 44% of phone companies have implemented the mandated anti-spoofing protocol
- **48% of illegal robocalls** carry the highest (A-Level) trust signature
- Technology fails against legacy copper TDM networks, which strip digital signatures entirely
- Providers authenticate the customer — but are not required to inspect content or intent

3.2 The FCC Enforcement Illusion

$208M	**$6,790**	**0.003%**
Fines Levied Since 2015	Actually Collected	Collection Rate

Financial penalties have become a cost of doing business — that is rarely paid. The FCC's new "nuclear option" (RMD purges) disconnects non-compliant providers from the grid but creates binary, disproportionate consequences for compliance failures.

3.3 The Looming Supreme Court Threat (April 2026)

An upcoming Supreme Court case threatens to further erode the FCC's enforcement capability. Building on the Fifth Circuit's *Jarkesy* ruling, the court is considering whether administrative fines by agencies like the FCC violate the Seventh Amendment right to a jury trial.

- **If upheld:** Every FCC fine would require a full federal jury trial
- The DOJ lacks resources to prosecute every robocall scammer or non-compliant carrier
- The FCC would be left only with the "sledgehammer" of network disconnection — no graduated fines
- Risk of critical 911 infrastructure outages if regional carriers are cut off

4 Byte Federal: Industry-Leading Fraud Prevention

While regulators and banks have failed to close the gap, Byte Federal has built a comprehensive, multi-layered fraud prevention system that directly addresses each stage of the scam chain

— identifying victims in real time, intervening before transactions complete, and protecting vulnerable populations.

Of customers over 60 identified as potential scam victims are **successfully prevented** from completing a fraudulent transaction.

4.1 Layer 1: Mandatory KYC and Identity Verification

Byte Federal's onboarding process applies banking-grade identity verification — the exact rigor that telecom providers are not legally required to follow:

- Government-issued ID verification required for all first-time users
- Identity verification linked to transaction history and behavioral patterns
- Biometric confirmation capabilities integrated at kiosk level
- Real-time identity cross-referencing against fraud databases

4.2 Layer 2: AI-Powered Real-Time Behavioral Detection

Byte Federal's kiosks deploy advanced AI safety systems that monitor the live transaction environment:

- Camera-based analysis detects coercion signals — urgent bill-feeding, phone script-reading, visible distress
- Machine learning models trained on known scam patterns flag anomalous activity
- Transaction pacing analysis identifies rushed, panic-driven behavior
- Automatic transaction halt capability when coercion patterns are detected

4.3 Layer 3: Kiosk Warnings and Mandatory Scam Education

Every Byte Federal kiosk incorporates mandatory, age-sensitive fraud warning systems:

- Prominent on-screen scam warnings displayed at transaction initiation
- Explicit warnings about government imposter, IRS, tech support, and grandparent scams
- Users must affirmatively confirm they are not acting under third-party instructions
- Warning language specifically tailored to senior customers
- QR codes and printed resources linking to scam education materials

4.4 Layer 4: Anti-Fraud Terms of Service

Byte Federal's Terms of Service create explicit, enforceable prohibitions against fraud facilitation:

- Explicit prohibition on transactions conducted under third-party direction
- Contractual obligation for users to confirm they are acting of their own free will
- Documented acknowledgment of common scam scenarios before high-risk transactions

- Right to decline or halt transactions at any point without penalty

4.5 Layer 5: Live Outreach Calls to Customers Over 60

Byte Federal's most distinctive fraud prevention tool is direct human intervention — a live phone call program targeting customers over 60:

Trigger	Intervention	Outcome
Customer over 60 initiates transaction flagged by AI behavioral or amount thresholds	Trained Byte Federal compliance team member calls the customer directly, in real time	**84%** of targeted customers over 60 are successfully prevented from completing a fraudulent transaction

The live call process includes:

- Friendly, non-confrontational fraud education specific to the scenario
- Direct questions about whether instructions were received by phone or online
- Offer to pause the transaction and involve a trusted family member
- Documented call records for SAR reporting and regulatory compliance
- Referral to law enforcement or adult protective services when fraud is confirmed

4.6 Fraud Prevention Metrics

Metric	Result
Prevention rate for customers over 60 (flagged)	**84%**
Legitimate transaction rate (industry-wide BTM)	**98.8%**
Illicit transaction rate (industry-wide BTM)	1.2%
Annual compliance investment vs. VoIP competitor	**5,000x more**

5 Banning Bitcoin ATMs Hurts the Most Vulnerable

Proposals to ban or severely restrict crypto ATMs would disproportionately harm the communities that depend on them most — while having minimal impact on fraud.

5.1 24.6 Million Unbanked Americans

Crypto ATMs serve as critical financial infrastructure for communities with limited banking access:

Demographic	Unbanked Rate
Native American households	12.2%
Black households	10.6%
Hispanic households	9.5%
White households	1.9%

Banning Bitcoin ATMs would remove a financial lifeline for these communities while criminals simply redirect victims to wire transfers, gift cards, or cash-by-mail — which collectively account for far more fraud losses.

5.2 Fraud in Context

Only **1.5% of total internet crime losses** involve crypto ATMs. The fraud landscape by payment method:

Payment Method	Fraud Losses
Check Fraud (Global)	$26.6B
Bank Transfers	$2.09B
Wire Transfers	$287M
Bitcoin ATMs	$246.7M

6 Conclusion: Stop the Signal, Stop the Theft

The $12.5 billion elder fraud crisis is not primarily a financial industry failure — it is a **telecommunications failure**. The phone call is the initiation. The payment is merely the symptom.

While regulators debate court cases and technology continues to be bypassed by copper wires and lazy attestation, the most effective interventions are happening at the financial endpoint — specifically at organizations like Byte Federal that have chosen to invest proactively in protection rather than waiting for regulatory mandates.

6.1 The Path Forward Requires Three Things

1. **Mandatory Telecom KYC:** Apply banking-grade Know Your Customer standards to VoIP providers — real identity verification, not just email addresses and filing fees.
2. **Financial Liability for Attestation Signers:** Carriers that grant A-Level trust to scammers should share liability for resulting losses, with bonds forfeited upon facilitation of fraud.
3. **Confirmation of Payee at the Bank Level:** Mandate recipient account name verification for wire transfers, as the UK has done — a proven 50% fraud reduction measure still absent in the United States.

Byte Federal has already built the gold standard of what fraud prevention looks like at the endpoint. The regulatory system now needs to build the same standard at the front door — the phone network where the crime actually begins.

ENFORCE EXISTING LAWS

The data is clear: banning crypto ATMs addresses a symptom while leaving the root cause — unregulated telecom — completely untouched. Enforce existing laws to stop the signal, rather than banning the bridge that serves 24 million Americans.

Sources: FBI Elder Fraud Reports | FCC Enforcement Actions | Robocall Mitigation Database | CFPB Research | YouMail Robocall Index | FTC Consumer Sentinel Report 2024 | FBI IC3 Elder Fraud Report 2024

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