ByteFederal

The Architecture of Exploitation

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

Prepared For:
Regulators, Policymakers, Law Enforcement & Press

Prepared By:
Byte Federal, Inc.
Venice, Florida

Date: March 2026
Version: 2.0

Contents

Executive Summary

At a Glance

Subject:	The $12.5 billion elder fraud crisis and its root cause
Core Thesis:	The fraud chain begins in telecom, not at cryptocurrency ATMs
Key Data:	52.5B robocalls; $4.9B elder losses; 98.8% of BTM transactions legitimate
Solution:	Enforce existing telecom KYC rules; mandate Confirmation of Payee
Audience:	Regulators, policymakers, law enforcement, and press

The $12.5 billion annual fraud crisis targeting American consumers — particularly seniors — is not primarily a financial industry failure. It is a **telecommunications failure**. Every data-driven analysis of the fraud chain reveals the same architecture: the crime begins with an inadequately regulated phone call and ends at a heavily regulated financial endpoint.

This report traces the complete five-stage scam architecture, documents the profound regulatory asymmetry between telecom and financial services, and presents Byte Federal's industry-leading fraud prevention framework — which achieves an **84% prevention rate** for targeted customers over 60.

$12.5B
Annual Fraud
Total consumer losses (2024)

52.5B
Robocalls
Received by Americans in 2025

84%
Prevention
Elder fraud prevention rate

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.

52.5 BILLION

Robocalls received by Americans in 2025 — the highest volume since 2019.[a]

[a]YouMail Robocall Index, Annual U.S. Robocall Volume Report (2025). YouMail's data is compiled from analysis of over 200 billion calls across its user base and is widely cited by the FCC, FTC, and major media outlets.

$12.5B	+43%	$4.9B
Total Fraud Losses (2024)[1]	Elder Fraud Surge (YoY)[2]	Reported Elder Losses[3]

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.[a]

[a] See AARP, National Elder Fraud Survey (2024) (estimating that fewer than 1 in 44 elder fraud cases is reported to authorities); see also U.S. Department of Justice, Elder Justice Initiative: The Scope of Elder Abuse (2023).

Phone calls remain the **primary fraud vector**, producing the highest median individual loss of any contact method:[4]

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

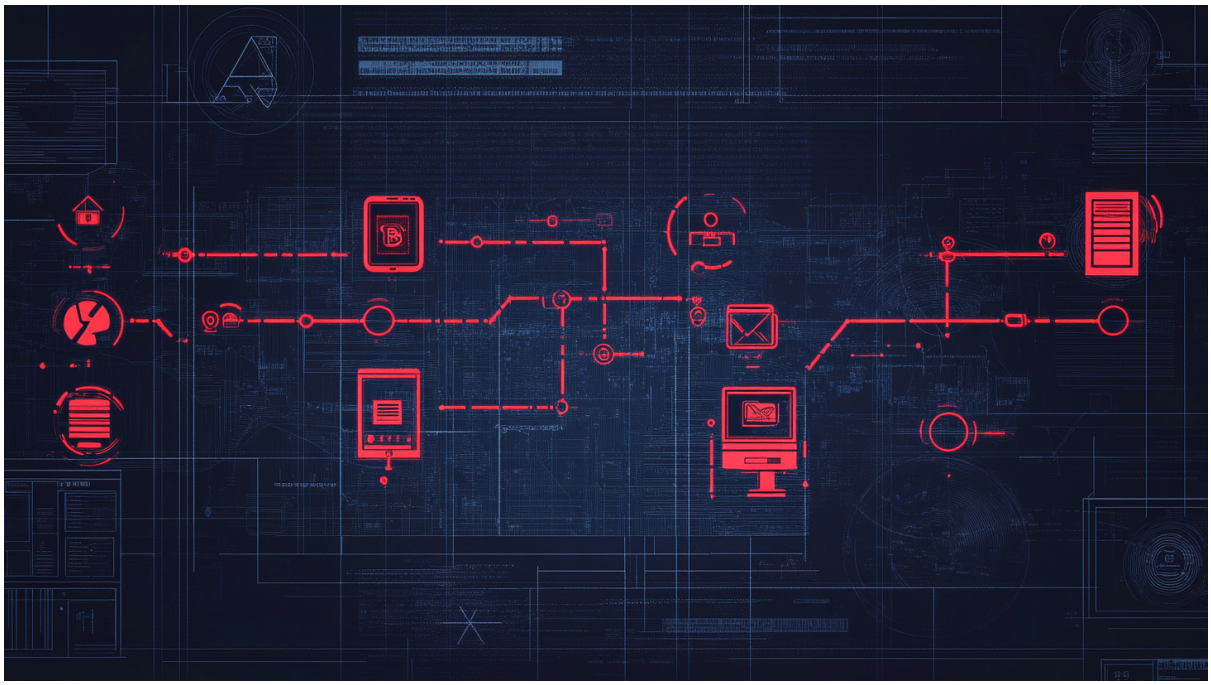
The concentration of losses in phone-initiated fraud underscores a critical structural point: the telecommunications system is the primary enabler. Regardless of the ultimate payment method — whether wire transfer, gift card, or cryptocurrency — the scam overwhelmingly begins with a phone call. **41% of high-loss senior scams** originate with a phone call,[5] which produces the highest median individual losses of any fraud vector at $2,210 per incident.

[4] FTC, Consumer Sentinel Network Data Book 2024, supra note 2. Contact method analysis based on reports where contact method was identified.

[5] FTC, Consumer Sentinel Network Data Book 2024, supra note 2 ("Older adults reported phone as the contact method in 41% of reports where the fraud resulted in losses over $1,000").

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.

KEY PRINCIPLE

We strictly regulate the **EXIT door** (banks, crypto ATMs) but leave the **FRONT DOOR** (telecom) inadequately enforced. 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. While FCC rules formally require providers to take "affirmative, effective measures" to prevent customers from using their networks to originate illegal calls — including "knowing its customers" and exercising due diligence[1] — compliance prior to 2025 was so poor that the FCC had never once enforced these obligations against a VoIP provider.[2] In practice, gaining access to the US telephone grid required little more than:

- $100 filing fee to the FCC Robocall Mitigation Database (RMD) — the only barrier to entry[3]
- No background checks, no surety bonds, no suspicious activity reports[4]
- Ineffective identity screening — fictional names, hotel addresses, and anonymous cryptocurrency payments were accepted as standard practice[5]

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.[a]

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

[a] In re Telnyx LLC, supra note 13. The FCC's enforcement action detailed how Telnyx's onboarding process failed to verify the identity, address, or business legitimacy of the registrant despite clear indicators of fraud.

[b] Operating as an unlicensed money transmitter is a federal felony under 18 U.S.C. § 1960. Banks are required to implement Customer Identification Programs (CIPs) under 31 C.F.R. § 1020.220, which mandate verification of identity through documentary and non-documentary methods before account opening.

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[6] — marking a historic but belated recognition of the problem. That the FCC waited until 2025 to bring its first KYC enforcement case — despite years of its own rules requiring

[1] 47 C.F.R. § 64.6305(b); FCC, Advanced Methods to Target and Eliminate Unlawful Robocalls, Third Report and Order, WC Docket No. 17-97, 36 FCC Rcd 7596 (2021).

[2] FCC Enforcement Bureau, Enforcement Advisory: Robocall Mitigation Database Non-Compliance (2025) (describing the first-ever KYC enforcement action against a VoIP provider).

[3] 47 C.F.R. § 64.6305 (requiring voice service providers to file a certification with the Robocall Mitigation Database). The filing fee structure is established by the FCC's registration requirements.

[4] Unlike Money Services Businesses registered with FinCEN under 31 U.S.C. § 5330, VoIP providers face no federal requirement for surety bonds, SAR filing, or background investigations of principals. Compare 31 C.F.R. § 1022.380 (MSB registration requirements including identification of ownership) with 47 C.F.R. § 64.6305 (VoIP certification requires only a description of robocall mitigation efforts).

[5] See In re Telnyx LLC, FCC File No. EB-TCD-22-00035822, Notice of Apparent Liability for Forfeiture, $4,500,000 (2025) (finding that Telnyx onboarded customers using aliases, temporary addresses, and unverified payment methods).

[6] In re Telnyx LLC, supra note 13. The $4.5 million proposed forfeiture was the FCC's first enforcement action specifically targeting a provider's failure to implement effective KYC procedures for VoIP customer onboarding.

providers to "know" their customers — speaks volumes about the depth of the regulatory failure.

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:[7]

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.[8]	Providers grant scammers the highest possible trust rating (A-Level attestation) based purely on having a billing relationship — without inspecting call content or intent.[9] 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.[10]

A critical nuance often missed in public debate: STIR/SHAKEN is an authentication framework, not a fraud detection system. It can verify whether a caller has the right to use a particular phone number, but it cannot determine whether the caller has fraudulent intent.[11] This means that even a perfectly implemented STIR/SHAKEN system would still allow scammers who have legitimately obtained phone numbers to make calls with the highest trust rating.

[7] FCC, Second Report and Order, WC Docket No. 17-97 (establishing the STIR/SHAKEN framework and robocall mitigation database requirements). Industry investment estimates are compiled from carrier filings and FCC implementation reports.

[8] FCC, STIR/SHAKEN Implementation: Status and Challenges, Report to Congress (2024). The FCC acknowledged that TDM network interoperability remains the "single largest gap" in the STIR/SHAKEN framework, affecting approximately 40% of call paths that traverse at least one TDM segment.

[9] U.S. Government Accountability Office, Caller ID Spoofing: FCC and FTC Actions and the Challenges of Enforcing Laws on Fake Caller ID Schemes, GAO (summary report) ("stakeholders cautioned that technical verification cannot determine whether a caller has fraudulent intent—it can only help verify whether the caller has the right to use the caller ID being transmitted").

[10] FCC, In re Lingo Telecom, LLC, File No. EB-TCD-24-00037347, Consent Decree, DA 24-453 (2024). Lingo Telecom agreed to a $1 million settlement for transmitting AI-generated robocalls with spoofed caller ID during the 2024 New Hampshire presidential primary.

[11] GAO, Caller ID Spoofing, supra note 19. This is the cleanest, citation-backed way to explain the limitation: scammers exploit a regime where caller-ID trust signals can be partially authenticated without solving for intent.

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

[a]Compiled from FCC Enforcement Bureau annual reports and fine collection data (2015–2025). The $208 million represents the total nominal value of Notices of Apparent Liability and Forfeiture Orders issued by the FCC for robocall and caller ID spoofing violations. The $6,790 in actual collections was confirmed through FCC responses to Congressional inquiries.

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.[12] 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

The FTC's new Government and Business Impersonation Rule, finalized in 2024, makes it explicitly unlawful to impersonate government agencies and businesses in interstate commerce.[13] However, enforcement remains challenging: identifying the source of spoofed calls is technically difficult, scammers are often based overseas, and jurisdictional complexity slows response.[14]

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.

[12]Caller ID spoofing is prohibited under the Truth in Caller ID Act when done "with the intent to defraud, cause harm, or wrongfully obtain anything of value." 47 U.S.C. § 227(e)(1). The statute specifically targets intent-based misuse rather than the mere technical act of altering caller ID. See FCC, Truth in Caller ID Act of 2009 — Rules and Regulations Implementing the Truth in Caller ID Act of 2009, Report and Order, 26 FCC Rcd 9114 (2011).

[13]FTC, Rule on Impersonation of Government and Businesses, 16 C.F.R. Part 461, 89 Fed. Reg. 15,072 (Mar. 1, 2024), effective Apr. 1, 2024. The rule allows the FTC to seek civil penalties and consumer redress for impersonation scams.

[14]GAO, Caller ID Spoofing, supra note 19 (noting that "enforcement can be challenging because it can be difficult to identify the source of spoofed calls and scammers may be based overseas").

2.4.1 What Federal Law Actually Requires

Understanding the bank's role requires separating two distinct regulatory obligations: Currency Transaction Reports (CTRs) and Suspicious Activity Reports (SARs).[15]

Under Treasury rules, each financial institution must file a CTR for each deposit, withdrawal, exchange of currency, or other payment or transfer involving **more than $10,000 in currency**.[16] CTRs must be electronically filed within 15 calendar days following the day the reportable transaction occurred.[17] Banks must verify and record identifying information for the person presenting the transaction — the FFIEC BSA/AML Manual is explicit that the notation "known customer" is prohibited as a substitute for identification detail.[18]

The bank SAR rule is a different trigger. A bank must file a SAR when a transaction involves or aggregates at least **$5,000**, and the bank "knows, suspects, or has reason to suspect" it involves illegal funds, evasion, or has no apparent lawful purpose.[19] SARs are also legally confidential: banks and their employees may not disclose a SAR or any information that would reveal the existence of a SAR.[20]

What Banks Are Required to Do	What Banks Are Not Required to Do
File CTRs for cash withdrawals over $10,000[21]	Deny access to funds based on suspected fraud
File SARs for transactions over $5,000[22]	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[23]	Halt a transaction because a senior is on their phone reading a script

2.4.2 The Critical Distinction: Reporting vs. Transaction Denial

The CTR rule is a reporting rule keyed to cash amount and transaction type. It does not say "stop the withdrawal." The SAR rule is a reporting rule keyed to suspicion and a $5,000 threshold. It does not say "you must deny the customer their cash."[24]

[15] See generally 47 U.S.C. § 227(e) (Truth in Caller ID Act); 31 C.F.R. §§ 1010.311, 1020.320 (CTR and SAR rules).

[16] 31 C.F.R. § 1010.311; 31 U.S.C. § 5313 (authorizing FinCEN's currency transaction reporting requirements). The obligation explicitly covers withdrawals.

[17] 31 C.F.R. § 1010.306(a)(1).

[18] FFIEC, Bank Secrecy Act / Anti-Money Laundering Examination Manual, "Currency Transaction Reporting" section, available at https://bsaaml.ffiec.gov/manual.

[19] 31 C.F.R. § 1020.320(a)(2). SARs must be filed no later than 30 calendar days after initial detection, with a limited extension when no suspect is identified.

[20] 31 C.F.R. § 1020.320(e). This confidentiality requirement is particularly relevant to the bank-stage critique: even if a bank files a SAR, it is legally constrained from "showing its work" to the customer or the public.

[21] 31 C.F.R. § 1010.311; 31 U.S.C. § 5313.

[22] 31 C.F.R. § 1020.320(a)(2).

[23] 31 C.F.R. § 1020.220 (Customer Identification Program requirements for banks).

[24] 31 C.F.R. §§ 1010.311, 1020.320 (read together, the rules establish reporting duties, not transaction-denial mandates). See also FFIEC, BSA/AML Examination Manual, "Suspicious Activity Reporting" section (describing SAR filing as a "critical internal control" but not as a basis for transaction refusal).

On elder financial exploitation, agencies have pushed banks toward stronger intervention strategies — but generally as guidance rather than a blanket new federal mandate. An interagency elder financial exploitation statement explicitly says it does **not** establish new regulatory requirements or supervisory expectations and does **not** set a compliance standard; it is intended to "raise awareness" and provide "strategies."[25] A summary posted by the Consumer Financial Protection Bureau lists strategies agencies are calling for, including employee training, transaction holds and disbursement delays "as appropriate" and consistent with applicable law, trusted contact processes, and timely SAR filing.[26]

The Senior Safe Act does not mandate action, but provides liability immunity for certain eligible employees and institutions that report suspected exploitation, conditioned on training and good-faith, reasonable-care reporting.[27]

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.[a]

[a] CFPB summary, supra note 37. Translated into plain English: intervention authority is often a mix of internal policy, supervisory expectations, and state-law options — combined with federal reporting obligations that do not necessarily stop the withdrawal by themselves.

2.4.3 The Missing Safeguard: Confirmation of Payee

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.[28] 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.[29]

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

[25] NCUA et al., Interagency Statement on Elder Financial Exploitation (2023), available at https://www.ncua.gov ("This statement does not establish new regulatory requirements or supervisory expectations...").

[26] CFPB, Interagency Guidance on Elder Financial Exploitation Prevention Strategies (summary), available at https://www.consumerfinance.gov.

[27] Senior Safe Act, 12 U.S.C. § 3423; SEC, Senior Safe Act Overview, Investor.gov, available at https://www.investor.gov.

[28] UK Payment Systems Regulator, Confirmation of Payee: Implementation and Impact Assessment (2024). CoP was mandated for the six largest UK banking groups in 2020 and extended to all payment service providers in 2024.

[29] FBI IC3, Internet Crime Report 2024 (reporting $2.09 billion in losses from business email compromise and wire transfer fraud). Compare with $246.7 million in reported losses involving cryptocurrency kiosks. See IC3, 2024 Elder Fraud Report, supra note 3.

the most heavily regulated financial entities in the United States:[30]

Bitcoin ATM Operators	VoIP Telecom Providers
AML Program — **Mandatory** 5-Pillar Framework[31]	AML Program — **NONE**
SARs — **Mandatory** for transactions over $2,000[32]	SARs — **NONE**
State Money Transmitter Licenses — **Required in ?48 states**[33]	State Licensing — Federal FCC only ($100 fee)
FinCEN Registration — **Mandatory** Federal[34]	FinCEN Registration — **NOT REQUIRED**
Surety Bonds — **Millions required** to operate[35]	Surety Bonds — **NONE**
Operating without license: **Federal Felony**[36]	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**.[37] Illicit activity accounts for only 1.2% — a reflection of rigorous compliance, not regulatory laxity.

[30] Bitcoin ATM operators are classified as Money Services Businesses (MSBs) under federal law and must register with FinCEN pursuant to 31 U.S.C. § 5330. They are further classified as money transmitters under most state laws, requiring individual state licenses. See FinCEN, Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies, FIN-2013-G001 (Mar. 18, 2013).

[31] 31 C.F.R. § 1022.210 (requiring MSBs to develop, implement, and maintain an effective anti-money laundering program including: (1) internal policies, procedures, and controls; (2) designation of a compliance officer; (3) ongoing employee training; (4) independent review; and (5) risk assessment).

[32] 31 C.F.R. § 1022.320(a)(2) (MSB SAR filing threshold of $2,000, compared to the $5,000 threshold for banks under § 1020.320).

[33] See, e.g., Fla. Stat. § 560.103 (Florida Money Services Business Act); N.Y. Banking Law § 641 (New York money transmitter licensing). Byte Federal holds active money transmitter licenses or equivalent registrations in 48 states.

[34] 31 U.S.C. § 5330; 31 C.F.R. § 1022.380 (requiring MSBs to register with FinCEN, including identification of ownership and agent information).

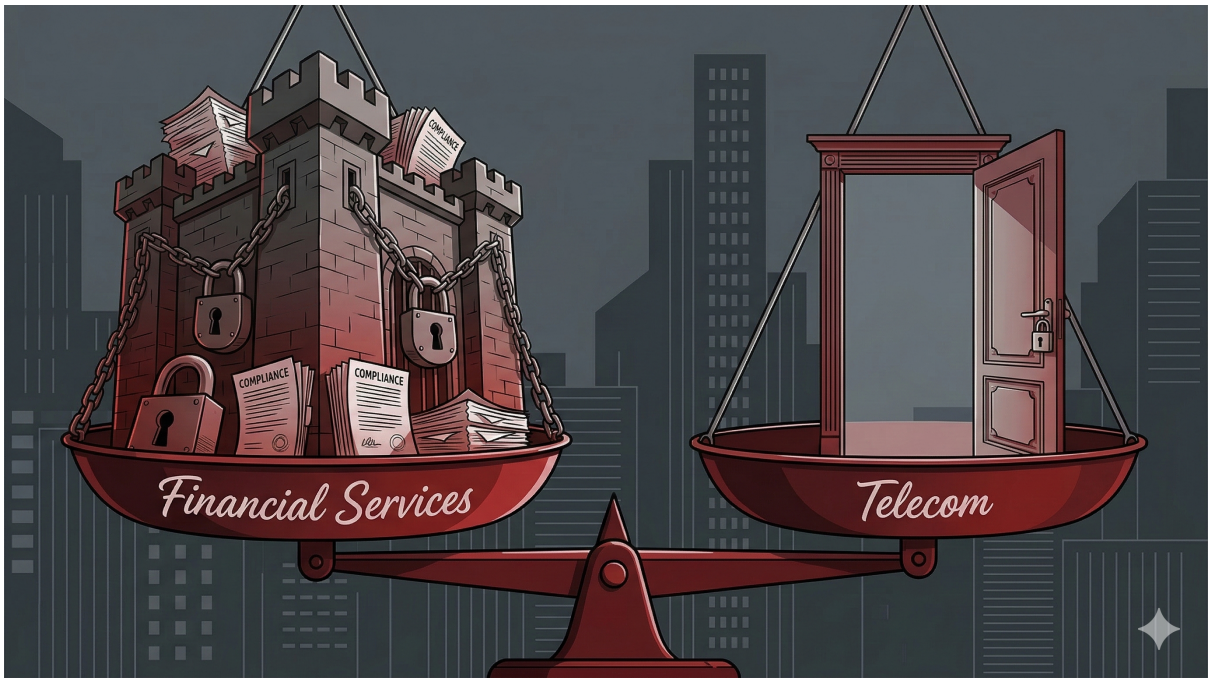
[35] State money transmitter licensing requirements typically include surety bond obligations. Bond amounts vary by state and transaction volume, often ranging from $100,000 to several million dollars. See, e.g., N.Y. Banking Law § 651 (bond requirements for New York licensees).

[36] 18 U.S.C. § 1960 (operating an unlicensed money transmitting business is punishable by up to 5 years imprisonment and fines).

[37] Chainalysis, 2024 Crypto Crime Report (2024). Chainalysis analyzed on-chain transaction data across the cryptocurrency ecosystem and found that illicit activity accounted for approximately 1.2% of total BTM transaction volume. A 2024 academic study corroborated this finding, noting that BTMs function as "AML data capture points" that integrate anonymous cash into the monitored financial system. See Hayashi & Routh, Cryptocurrency Ownership and Use: A Federal Reserve Bank of Kansas City Working Paper (2024/2025).

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.

THE PARADOX

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 — inadequately enforced.

3.1 The STIR/SHAKEN Technology Failure

- $250 million invested in STIR/SHAKEN caller authentication technology[1]
- Only 44% of phone companies have implemented the mandated anti-spoofing protocol[2]
- **48% of illegal robocalls** carry the highest (A-Level) trust signature[3]
- Technology fails against legacy copper TDM networks, which strip digital signatures entirely[4]
- Providers authenticate the customer — but are not required to inspect content or intent[5]

3.2 The FCC Enforcement Illusion

$208M	$6,790	0.003%
Fines Levied Since 2015[6]	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. In 2025, the FCC Enforcement Bureau removed providers from the Robocall Mitigation Database and described removal as preventing those providers from connecting with U.S. networks until compliance, while emphasizing STIR/SHAKEN certification and robocall mitigation obligations.[7] Later that same period, the FCC announced it had removed over 1,200 non-compliant providers from the database, describing this as effectively disconnecting them from the U.S. phone network until compliance.[8]

Those enforcement actions matter rhetorically because they support a fact-based provocation: if the regulatory framework already recognizes that upstream telecom providers can be a major choke point for fraud and robocalls, why is the public

[1] FCC, Second Report and Order, WC Docket No. 17-97, supra note 17. The $250 million estimate encompasses carrier implementation costs as reported in industry filings and FCC cost-benefit analyses.

[2] FCC, Robocall Mitigation Database: Provider Compliance Report (2025). Of approximately 5,000 registered voice service providers, fewer than half had achieved full STIR/SHAKEN implementation as of Q4 2024.

[3] TransNexus, STIR/SHAKEN Effectiveness Analysis (2025); see also FCC, STIR/SHAKEN Implementation Report, supra note 18. The A-Level trust paradox occurs because attestation levels are based on the provider's relationship with the customer, not on the legitimacy of the call content.

[4] FCC, STIR/SHAKEN Implementation Report, supra note 18 (acknowledging that "calls traversing TDM network segments cannot carry STIR/SHAKEN attestation information").

[5] GAO, Caller ID Spoofing, supra note 19. "Technical verification cannot determine whether a caller has fraudulent intent — it can only help verify whether the caller has the right to use the caller ID being transmitted."

[7] FCC Enforcement Bureau, Enforcement Advisory: Robocall Mitigation Database Non-Compliance, supra note 9.

[8] FCC, FCC Removes Over 1,200 Non-Compliant Providers from Robocall Mitigation Database (2025 press release).

narrative so often fixated on the last-mile cash-to-crypto endpoint?[9]

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.[10]

- **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

The practical impact is stark: if the FCC can no longer levy administrative fines — its already-ineffective primary tool — and must instead rely on DOJ prosecution for each enforcement action, the regulatory regime collapses from inadequate to functionally non-existent.

[9] See 47 C.F.R. § 64.6305; FCC Robocall Mitigation Database enforcement actions (2025), supra notes 59–60.

[10] SEC v. Jarkesy, 603 U.S. ___ (2024). The Supreme Court held 6–3 that the SEC's use of in-house administrative proceedings to impose civil penalties for securities fraud violated the Seventh Amendment. The reasoning may extend to other agencies, including the FCC, that impose monetary penalties through administrative adjudication.

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.

84% PREVENTION RATE

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

[a]Byte Federal, Inc., internal compliance data (2024–2025). The 84% prevention rate is calculated from outcomes of the live outreach call program described in Section 4.5, tracking flagged transactions for customers aged 60 and older where a compliance team member made direct contact.

Byte Federal spearheaded a revision to the Florida Money Transmitter Laws in 2022, and because of this involvement, the state of Florida reached out to Byte Federal to help create policies and procedures for the entire virtual currency kiosk industry that Florida could adopt and mandate all operators to implement.[1]

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:[2]

- Government-issued ID verification required for all first-time users, regardless of transaction amount
- Selfie-to-ID photo comparison for biometric confirmation at kiosk level
- Identity verification linked to transaction history and behavioral patterns
- Real-time identity cross-referencing against fraud databases and OFAC screening[3]
- SSN collection and percentage-match verification for enhanced identity confirmation

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

[1]Byte Federal, Inc., Scam Deterrents, Counter Measures, and Due Diligence, Letter to the Florida Office of Financial Regulation (July 11, 2024). See also Fla. Stat. § 560.103 (as amended, June 2022, incorporating provisions recommended by industry participants including Byte Federal).

[2]Byte Federal's KYC process exceeds the Customer Identification Program (CIP) requirements applicable to banks under 31 C.F.R. § 1020.220, incorporating additional biometric and behavioral verification layers.

[3]Office of Foreign Assets Control (OFAC) screening is conducted at onboarding and monthly for all active customers with $10,000 or more in monthly transaction volume. See 31 C.F.R. Part 501 (OFAC regulations).

- 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 that must be acknowledged before any transaction can proceed:

- Prominent on-screen scam warnings displayed at transaction initiation, requiring 30-second acknowledgment period with randomized button placement to prevent reflexive dismissal[4]
- 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
- Multiple automated text messages warning about common scam scenarios sent following registration[5]
- 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 transacting to their own wallet, under their own control
- Documented acknowledgment of common scam scenarios before high-risk transactions
- Users found to have transacted using a wallet that is not their own are permanently blocked from the platform[6]
- Right to decline or halt transactions at any point without penalty

[4] Byte Federal, Inc., Scam Deterrents, supra note 65. The warning screen lists specific scam scenarios and requires customers to wait 30 seconds before the "I Understand This" acknowledgment button appears. Yes/No buttons are periodically repositioned to require active reading.

[5] Byte Federal, Inc., Scam Deterrents, supra note 65. Two separate SMS messages are sent post-registration: the first warns against third-party wallet use, and the second enumerates specific scam scenarios including government impersonation, job offerings, foreign lottery, and "relative in need" schemes.

[6] Byte Federal, Inc., Scam Deterrents, supra note 65. "If a user is found at any point to have transacted using a wallet that is not their own, whether through compliance due diligence or via a recorded support call, they are blocked from further use of our services."

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:[7]

- 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)[8]	**98.8%**
Illicit transaction rate (industry-wide BTM)	1.2%
Annual compliance investment vs. VoIP competitor	**5,000x more**

[7] Byte Federal, Inc., Scam Deterrents, supra note 65. "Account holds until support call with user if age 60 or older. Verbal confirmation that the user is not being scammed, is using own wallet, and multiple other-directed questions to instruct user of scams."

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. According to the FDIC's 2023 National Survey of Unbanked and Underbanked Households — 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 households, are classified as underbanked.[2] Cumulatively, 18.4% of American households (roughly 24.6 million) remain structurally outside the mainstream financial ecosystem.

Unbanked Rates by Demographics

12.2%	Native American households[a]
10.6%	Black households
9.5%	Hispanic households
1.9%	White households

Financial exclusion is highly correlated with race, income, educational attainment, and disability status. Among households earning less than $15,000 annually, the unbanked rate surges to 21.8%.[3] Households headed by an individual lacking a high school diploma face a 19.7% unbanked rate — nearly 25 times higher than the 0.8% rate among college graduates.[4] Between 2019 and 2023, the United States witnessed a 5.6% decline in physical bank locations, amounting to 5,413 branch closures; 3,629 census tracts now qualify as "banking deserts," leaving 12.3 million Americans without adequate branch access.[5]

For the 66.2% of unbanked households that rely entirely on physical cash for all transactions, online cryptocurrency exchanges that mandate linked checking accounts are completely inaccessible.[6] Bitcoin ATMs are 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.

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.[7]

5.2 Fraud in Context

Only **1.5% of total internet crime losses** involve crypto ATMs.[8] The fraud landscape by payment method:

[1] Federal Deposit Insurance Corporation, 2023 National Survey of Unbanked and Underbanked Households (Oct. 2024). In these households, no individual maintains a checking or savings account at a federally insured depository institution.

[2] Id. Underbanked households technically possess a bank account but remain functionally marginalized, actively relying on nonbank alternative financial services such as money orders, check-cashing services, and payday loans.

[3] FDIC, 2023 National Survey, supra note 77.

[4] Id.

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

[6] FDIC, 2023 National Survey, supra note 77 (reporting that 66.2% of unbanked households use only cash for day-to-day transactions).

[7] FTC, Consumer Sentinel Network Data Book 2024, supra note 2 (reporting that wire transfers, gift cards, and cash/mail collectively accounted for over $4 billion in fraud losses in 2024, compared to $246.7 million involving cryptocurrency kiosks).

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

Payment Method	Fraud Losses
Check Fraud (Global)[9]	$26.6B
Bank Transfers[10]	$2.09B
Wire Transfers[11]	$287M
Bitcoin ATMs[12]	$246.7M

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.

If regulators and advocacy groups truly want to protect seniors, the question they must ask is: why is the loudest political energy directed at the last stop — after the spoofed contact and the bank cash-out — when telecom rules and bank-stage intervention guidance already describe upstream choke points that could slow or stop the scam earlier?[1]

[1] See 47 C.F.R. § 64.6305 (telecom KYC obligations); CFPB, Interagency Guidance on Elder Financial Exploitation Prevention Strategies, supra note 37 (bank-stage intervention strategies).

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. The FCC's rules already require providers to "know their customers" and take "affirmative, effective measures" to prevent illegal calls[2] — the problem is not the absence of rules but the absence of enforcement.[3]
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. The A-Level trust paradox — where 48% of illegal robocalls carry the highest trust rating[4] — exists because providers face no financial consequences for careless attestation.
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.[5]

THE BOTTOM LINE

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 — inadequately enforced telecom — completely untouched. Enforce existing laws to stop the signal, rather than banning the bridge that serves 24 million Americans.

[2] 47 C.F.R. § 64.6305(b), supra note 8.
[3] See In re Telnyx LLC, supra note 13 (first-ever KYC enforcement action, issued in 2025 despite the rule existing since 2021).
[4] TransNexus, supra note 56.
[5] UK Payment Systems Regulator, supra note 41.

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

[1] 12 U.S.C. § 3423 (Senior Safe Act)

[2] 15 U.S.C. § 45 (FTC Act — Unfair or Deceptive Acts or Practices)

[3] 18 U.S.C. § 1960 (Unlicensed Money Transmitting Business)

[4] 31 U.S.C. § 5313 (Reports on Domestic Coins and Currency Transactions)

[5] 31 U.S.C. § 5330 (Registration of Money Transmitting Businesses)

[6] 47 U.S.C. § 227(e) (Truth in Caller ID Act of 2009)

A.2 Federal Regulations (Code of Federal Regulations)

[7] 16 C.F.R. Part 310 (Telemarketing Sales Rule)

[8] 16 C.F.R. Part 461 (Rule on Impersonation of Government and Businesses)

[9] 31 C.F.R. § 1010.306(a)(1) (CTR Filing Deadline)

[10] 31 C.F.R. § 1010.311 (Currency Transaction Report Requirements)

[11] 31 C.F.R. § 1020.220 (Customer Identification Program — Banks)

[12] 31 C.F.R. § 1020.320 (Suspicious Activity Report — Banks)

[13] 31 C.F.R. § 1022.210 (Anti-Money Laundering Program — MSBs)

[14] 31 C.F.R. § 1022.320 (Suspicious Activity Report — MSBs)

[15] 31 C.F.R. § 1022.380 (MSB Registration Requirements)

[16] 31 C.F.R. Part 501 (OFAC Regulations)

[17] 47 C.F.R. § 64.6305 (Robocall Mitigation Database Requirements)

A.3 State Statutes

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

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

[20] N.Y. Banking Law § 651 (Surety Bond Requirements)

A.4 Court Cases

[21] SEC v. Jarkesy, 603 U.S. ___ (2024) (Seventh Amendment right to jury trial for administrative penalties)

A.5 FCC Orders, Enforcement Actions & Reports

[22] FCC, Truth in Caller ID Act of 2009 — Rules and Regulations Implementing the Truth in Caller ID Act of 2009, Report and Order, 26 FCC Rcd 9114 (2011)

[23] FCC, Advanced Methods to Target and Eliminate Unlawful Robocalls, Third Report and Order, WC Docket No. 17-97, 36 FCC Rcd 7596 (2021)

[24] FCC, Second Report and Order, WC Docket No. 17-97 (STIR/SHAKEN Framework and Robocall Mitigation Database Requirements)

[25] FCC, STIR/SHAKEN Implementation: Status and Challenges, Report to Congress (2024)

[26] FCC, Robocall Mitigation Database: Provider Compliance Report (2025)

[27] FCC Enforcement Bureau, Enforcement Advisory: Robocall Mitigation Database Non-Compliance (2025)

[28] FCC, FCC Removes Over 1,200 Non-Compliant Providers from Robocall Mitigation Database (2025 press release)

[29] In re Telnyx LLC, FCC File No. EB-TCD-22-00035822, Notice of Apparent Liability for Forfeiture, $4,500,000 (2025)

[30] In re Lingo Telecom, LLC, File No. EB-TCD-24-00037347, Consent Decree, DA 24-453 (2024)

[31] FCC Enforcement Bureau Annual Reports and Fine Collection Data (2015–2025) (compiled)

A.6 FTC Rules & Enforcement

[32] FTC, Rule on Impersonation of Government and Businesses, 16 C.F.R. Part 461, 89 Fed. Reg. 15,072 (Mar. 1, 2024), effective Apr. 1, 2024

[33] FTC, Consumer Sentinel Network Data Book 2024 (Feb. 2025)

A.7 Government Reports & Data

[34] Federal Bureau of Investigation, Internet Crime Complaint Center (IC3), Internet Crime Report 2024

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

[36] U.S. Government Accountability Office, Caller ID Spoofing: FCC and FTC Actions and the Challenges of Enforcing Laws on Fake Caller ID Schemes, GAO Summary Report

[37] U.S. Department of Justice, Elder Justice Initiative: The Scope of Elder Abuse (2023)

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

[39] FFIEC, Bank Secrecy Act / Anti-Money Laundering Examination Manual, available at https://bsaaml.ffiec.gov/manual

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

[41] NCUA et al., Interagency Statement on Elder Financial Exploitation (2023)

[42] CFPB, Interagency Guidance on Elder Financial Exploitation Prevention Strategies (summary)

[43] SEC, Senior Safe Act Overview, Investor.gov

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

A.8 Industry Research & Analysis

[45] YouMail Robocall Index, Annual U.S. Robocall Volume Report (2025)

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

[47] TransNexus, STIR/SHAKEN Effectiveness Analysis (2025)

[48] Hayashi & Routh, Cryptocurrency Ownership and Use: A Federal Reserve Bank of Kansas City Working Paper (2024/2025)

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

[50] AARP, National Elder Fraud Survey (2024)

A.9 Byte Federal Sources

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

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