ByteFederal

Closing the Telecom Regulatory Gap

How Caller ID Spoofing, Unenforced FCC Rules, and Bank Reporting Gaps Enable Elder Fraud

Prepared For:
Regulators, Policymakers, Law Enforcement & Press

Prepared By:
Byte Federal, Inc.
Venice, Florida

Date: March 2026
Version: 1.0

CONFIDENTIAL

Contents

Executive Summary

At a Glance

Subject:	The telecom regulatory gaps that enable elder fraud
Core Thesis:	FCC rules exist but are unenforced; bank reporting rules create documentation, not intervention
Key Data:	$208M fines levied / $6,790 collected / 0.003% rate; 48% of illegal calls carry A-Level trust
Solution:	Enforce existing telecom KYC; mandate Confirmation of Payee; close TDM bypass
Audience:	Regulators, policymakers, law enforcement, and press

Senior-targeted fraud that ends in cash-to-crypto payments is often described as a "Bitcoin ATM problem." But if you follow the chain of custody of the scam — from the spoofed call or text to the cash leaving a bank — you run into two heavily regulated systems that often escape the same level of public scrutiny: the U.S. telecom ecosystem and the U.S. banking reporting regime.

This report documents the specific regulatory gaps in telecommunications enforcement and bank reporting that allow elder fraud to persist — and presents actionable recommendations for closing them at the source rather than at the endpoint.

The regulatory gaps are specific and identifiable:

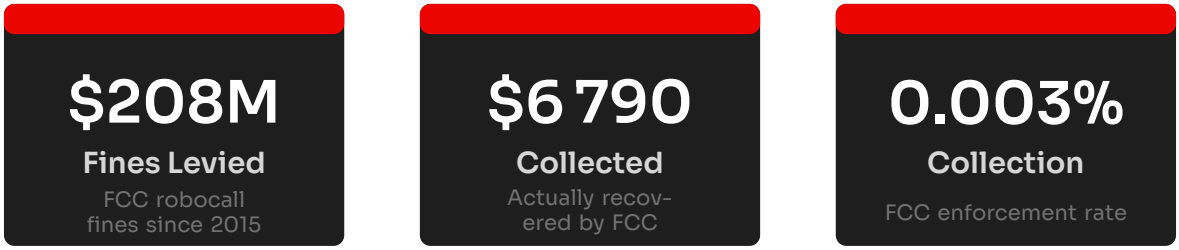
1. **Telecom KYC rules exist but were never enforced until 2025.** The FCC's own regulations require providers to "know their customers" and take "affirmative, effective measures" to prevent illegal calls — yet the first enforcement action did not arrive until 2025.
2. **STIR/SHAKEN authenticates numbers, not intent** — and fails entirely on legacy TDM networks. After hundreds of millions of dollars in industry investment, 48% of illegal robocalls still carry A-Level trust ratings.
3. **The FCC collects 0.003% of its fines**, and the Supreme Court's Jarkesy decision may eliminate administrative fining authority altogether.
4. **Bank CTR/SAR rules create reporting obligations, not transaction-denial man-**

dates. A $10,000+ cash withdrawal triggers a CTR filing — not a requirement to stop the withdrawal.

5. **No Confirmation of Payee exists in the United States**, despite the UK system reducing related fraud cases by nearly 60% since its 2020 launch, with annual APP fraud declining 17% in 2023.

Closing these gaps requires upstream enforcement — not downstream bans. The telecom regulatory gap is where the fraud enters the system. **Close it there.**

The analysis that follows provides the legal citations, enforcement data, and regulatory architecture behind each of these findings.



1

Introduction: The Upstream Problem

Where the Fraud Chain Actually Begins

Senior-targeted fraud that ends in cash-to-crypto payments is often described as a "Bitcoin ATM problem." But if you follow the chain of custody of the scam — from the spoofed call or text to the cash leaving a bank — you run into two heavily regulated systems that often escape the same level of public scrutiny: the U.S. telecom ecosystem and the U.S. banking reporting regime.[1]

This report focuses on two areas: (1) FCC/FTC rules on caller ID spoofing and telecom "verification" obligations, and (2) bank reporting requirements and what tellers are actually required — and not required — to do when a customer withdraws large

[1] 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).

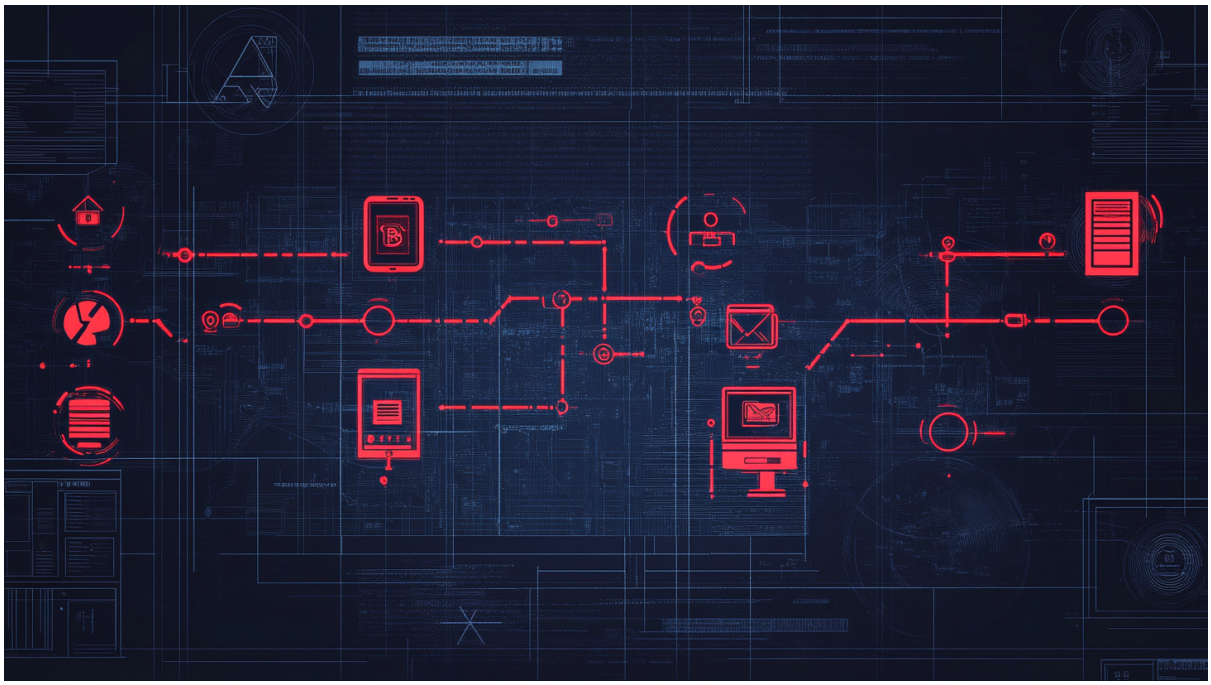
amounts of cash.[2]

The purpose is not to assign blame but to describe the regulatory architecture with precision — so that policy conversations focus on the structural gaps that enable fraud rather than the financial endpoints that terminate it.

[2] 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).

Caller ID Spoofing: What the Law Actually Says

Intent-Based Prohibition, Not a Blanket Ban



2.1 Spoofing Is Illegal in a Specific Way, Not as a Blanket Concept

U.S. law does not treat "spoofing" as automatically illegal. The core federal prohibition is narrower: it is unlawful to cause caller ID information to be misleading or inaccurate **when done with the intent to defraud, cause harm, or wrongfully ob-**

tain anything of value.[1] That standard applies in connection with voice service and text messaging service, and it also applies to actors outside the United States if the recipient is in the United States.[2]

The FCC implemented the Truth in Caller ID Act by adopting rules that track that same intent-based framework — targeting spoofing used for fraud, harm, or value, rather than outlawing every technical use of altered caller ID. The FCC's implementation took effect in 2011.[3]

Two implications matter:

First, "why doesn't the FCC just ban spoofing?" is partly answered by the statute itself: Congress designed the law around malicious intent, not around the existence of caller-ID manipulation as a technical capability.[4]

Second, even when the underlying conduct is plainly illegal — spoofing used to impersonate a bank, government agency, or family member to coerce a payment — enforcement can be difficult, slow, and jurisdictionally messy, especially when the source is hard to identify or is located overseas.[5]

[1] 47 U.S.C. § 227(e)(1). The statute defines the prohibited conduct in terms of harmful intent rather than the mere technical act of altering caller ID information.

[2] Id.

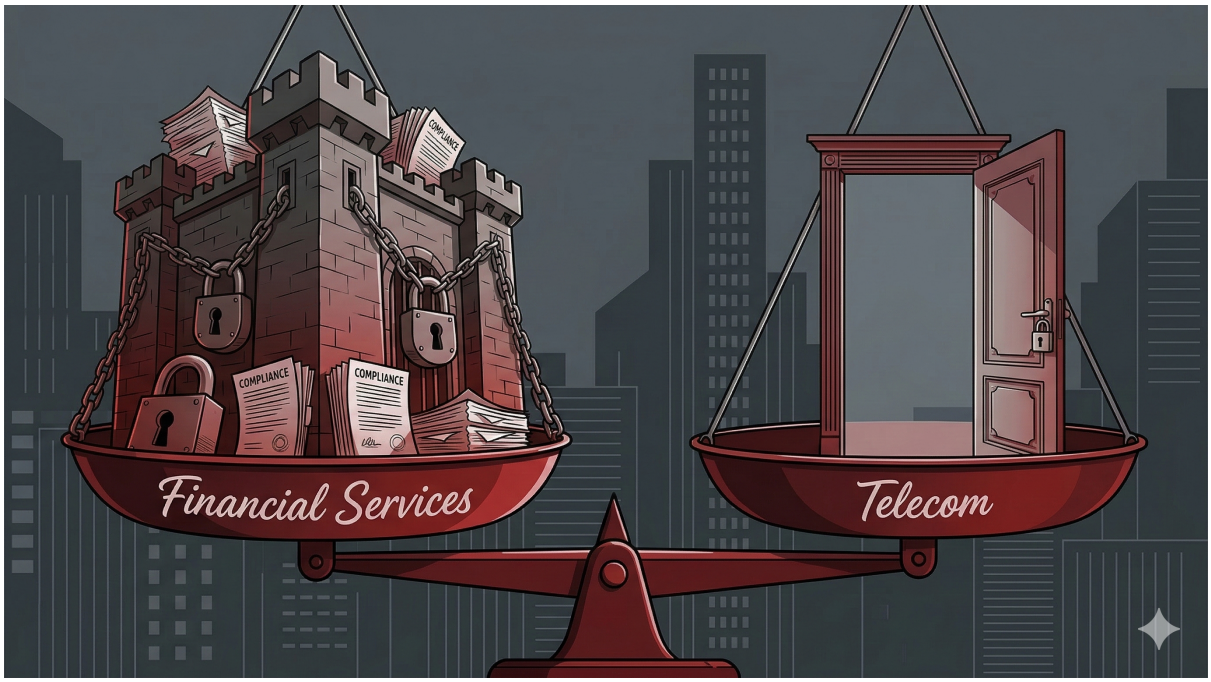
[3] FCC, Truth in Caller ID Act of 2009 — Rules and Regulations Implementing the Truth in Caller ID Act of 2009, Report and Order, 26 FCC Rcd 9114 (2011).

[4] 47 U.S.C. § 227(e)(1) (providing a carve-out for spoofing without fraudulent or harmful intent, such as law enforcement or certain privacy uses).

[5] GAO, Caller ID Spoofing, supra note 1 (describing enforcement challenges, including difficulty identifying call origins and overseas actors).

Telecom “Verification” Obligations

Real, But Uneven and Not a Silver Bullet



If you want to describe the telecom side precisely, you need to separate three layers: (a) the “this is illegal” layer (Truth in Caller ID), (b) the “authenticate and mitigate” layer (call authentication and robocall mitigation requirements), and (c) the “know your customer” style obligations placed on providers.

3.1 Robocall Mitigation and Traffic Gating Requirements

FCC rules require voice service providers to implement an “appropriate robocall mitigation program,” including reasonable steps to avoid originating illegal robocall traffic and a commitment to respond within 24 hours to traceback requests

from the FCC, law enforcement, and the industry traceback consortium.[1]

The rules also tie compliance to network access. Under the FCC's Robocall Mitigation Database framework, providers in the call path are required to accept or continue traffic only from providers whose certification appears in the database and has not been de-listed due to enforcement. The rule text explicitly sets conditions on accepting traffic from domestic providers, and it includes specific requirements for foreign providers and gateway providers.[2]

3.2 "Know Your Customer" Style Obligations for Telecom Providers

One of the most under-discussed elements in public debate is that FCC rules tell providers — explicitly — to take steps that look a lot like "KYC" for communications.

A provider must "take affirmative, effective measures to prevent new and renewing customers from using its network to originate illegal calls," including "knowing its customers" and exercising due diligence so that its services are not used to originate illegal traffic.[3]

The same rule set also pushes providers to monitor risk from upstream sources by requiring "reasonable and effective steps" to ensure that any originating or intermediate provider from which they directly receive traffic is not using the provider to carry or process a high volume of illegal traffic onto U.S. networks.[4]

This is the part of the story that cleanly supports a "front line" framing: there is a regulatory expectation that telecom providers perform customer due diligence and traffic-risk management to reduce illegal activity before it reaches consumers.[5]

3.3 FCC Enforcement Shows the Compliance Regime Is Still Leaky

The FCC's own actions underscore that compliance gaps are not theoretical. 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.[6]

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.[7]

[1] 47 C.F.R. § 64.6305; FCC, Second Report and Order, WC Docket No. 17-97 (robocall mitigation database and STIR/SHAKEN framework).

[2] Id. The database requirement creates a gating mechanism: non-certified providers lose interconnection access until compliance is restored.

[3] 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).

[4] Id. § 64.6305(c).

[5] Id.

[6] FCC Enforcement Bureau, Enforcement Advisory: Robocall Mitigation Database Non-Compliance (2025) (describing provider removals and network access consequences).

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

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 narrative so often fixated on the last-mile cash-to-crypto endpoint?[8]

[8] Id.

4

The FCC vs. FTC Jurisdictional Split

Divided Authority, Exploitable Gaps

4.1 The FTC's Role: Fraud and Impersonation Enforcement

It is accurate to say the FTC is active in enforcement around fraudulent calling behavior — but the FTC's control is not the same as controlling caller ID signaling itself.

The FTC's Telemarketing Sales Rule and related consumer protection authorities are a major enforcement toolset for scam calls and robocalls tied to telemarketing practices.[1]

Separately, the FTC finalized a rule prohibiting impersonation of government and businesses (and their officials and agents) in interstate commerce, effective April 1, 2024. This is aimed at the content and deception of the scam — impersonation — not the technical caller-ID mechanics.[2]

4.2 The Practical Division

The FTC can go after impersonators and deceptive actors (and can seek remedies and punitive tools tied to rule violations), while the FCC is the central actor for the caller-ID spoofing prohibition and the telecom compliance regime around mitigation and authentication.[3]

[1] 16 C.F.R. Part 310 (Telemarketing Sales Rule); FTC Act, 15 U.S.C. § 45 (unfair or deceptive acts or practices authority).

[2] 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.

[3] Id.; 47 U.S.C. § 227(e).

JURISDICTIONAL VULNERABILITY

The FCC owns the plumbing (caller ID authentication, provider compliance, network access). The FTC owns the content (impersonation, deception, consumer protection). Neither agency alone has both the technical authority and the enforcement resources to close the gap. This jurisdictional split is itself a structural vulnerability that scammers exploit.

The STIR/SHAKEN Failure

Technical Authentication ≠ Fraud Detection

A critical nuance — useful both for accuracy and for persuasion — is that technical authentication is not the same thing as fraud detection.

5.1 What STIR/SHAKEN Can and Cannot Do

A U.S. Government Accountability Office summary of federal efforts to combat fake caller ID schemes makes three points that translate cleanly into a public-interest narrative.

It notes spoofing is “in many cases illegal” and is used in schemes to obtain money and personal information, and characterizes spoofing complaints to the FCC and

FTC as suggesting a growing issue.[1]

It also highlights that enforcement can be challenging because it can be difficult to identify the source of spoofed calls and scammers may be based overseas.[2]

Most importantly for messaging discipline, it reports that 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.[3]

THE AUTHENTICATION GAP

Authentication can help verify whether a caller has the right to use a number, but it cannot read intent. That is why spoofing and impersonation keep working as social engineering even in a world with more call authentication.[a]

[a] GAO, Caller ID Spoofing, supra note 1.

5.2 The Numbers Tell the Story

STIR/SHAKEN Metric	Value
Investment in caller ID authentication[4]	Hundreds of millions
Phone companies implementing the protocol[5]	44%
Illegal robocalls carrying A-Level trust[6]	48%
FCC fines levied for robocall violations (since 2015)[7]	$208 million
FCC fines actually collected[8]	$6,790
Collection rate	0.003%

[1] GAO, Caller ID Spoofing, supra note 1.

[2] Id.

[3] Id. This distinction is critical: STIR/SHAKEN and similar authentication frameworks attest to number authorization, not caller intent.

[4] FCC, Second Report and Order, WC Docket No. 17-97, supra note 8 (industry implementation cost estimates from carrier filings).

[5] FCC, Robocall Mitigation Database: Provider Compliance Report (2025). (This figure reflects the count of registered providers, not percentage of call traffic; major carriers apply STIR/SHAKEN to approximately 86% of traffic by volume.)

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

[7] Compiled from FCC Enforcement Bureau annual reports and fine collection data (2015–2019, per a 2019 Wall Street Journal FOIA investigation; updated totals through 2025 are not publicly compiled, though the structural collection problem persists).

[8] Id.

Bank Reporting Requirements

What the Rules Actually Require

When discussing SARs and CTRs, it is important to get the threshold logic and what this does and does not force a teller to do exactly right.

6.1 CTRs for Cash Withdrawals Over $10,000

Under Treasury rules, each financial institution (other than casinos) must file a report of each deposit, withdrawal, exchange of currency, or other payment or transfer involving **more than $10,000 in currency**. That obligation explicitly covers withdrawals.[1]

The filing deadline for a CTR is within 15 days following the day the reportable transaction occurred.[2]

The FFIEC BSA/AML Manual adds operational detail that matters for teller-stage reality. It describes CTR filing as mandatory for currency transactions over $10,000 "by, through, or to the bank," and specifies that CTRs must be electronically filed within 15 calendar days after the transaction date.[3]

It states banks must verify and record identifying information for the person presenting the transaction — and it explicitly says the notation "known customer" is prohibited as a substitute for identification detail.[4]

It emphasizes aggregation: multiple currency transactions totaling more than $10,000 in cash-in or cash-out during one business day must be treated as a single transaction if the bank has knowledge they are conducted by or on behalf of any person, and branch transactions must be aggregated at the bank level.[5]

[1] 31 C.F.R. § 1010.311; 31 U.S.C. § 5313 (authorizing FinCEN's currency transaction reporting requirements).

[2] 31 C.F.R. § 1010.306(a)(1).

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

[4] Id.

[5] Id.

The punchline: a $10,000+ cash withdrawal is not just "a big withdrawal." It is a legally reportable cash event, with required recordkeeping and a filing obligation behind the scenes.[6]

6.2 SARs for Suspicious Activity

The bank SAR rule is a different trigger. A bank must file a SAR when a transaction is conducted or attempted by or through the bank, 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 (among other criteria).[7]

Timing is specific: a bank must file a SAR no later than 30 calendar days after initial detection (with a limited extension when no suspect is identified), and in some cases must notify law enforcement immediately by telephone in addition to filing.[8]

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, subject to narrow authorized sharing.[9]

That confidentiality point 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 to the public in real time.[10]

6.3 What Is Mandatory vs. What Is Not

THE CRITICAL DISTINCTION

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." CTR/SAR regimes create documentation, monitoring, and reporting obligations; they do not automatically compel transaction denial.[a]

[a] 31 C.F.R. §§ 1010.311, 1020.320 (read together, the rules establish reporting duties, not transaction-denial mandates).

6.4 The Elder Exploitation Guidance Landscape

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**

[6] 31 C.F.R. § 1010.311; 31 U.S.C. § 5313.
[7] 31 C.F.R. § 1020.320(a)(2).
[8] Id. § 1020.320(b)(3).
[9] Id. § 1020.320(e).
[10] Id.

set a compliance standard.[11]

- The CFPB 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.[12]
- 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.[13]

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.[14]

[11] 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…").

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

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

[14] CFPB summary, supra note 42.

7

The Jarkesy Threat

Administrative Fines Under Constitutional Challenge

The Supreme Court's 2024 Jarkesy decision is further eroding the FCC's already-inadequate enforcement capability.

In SEC v. Jarkesy, 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 right to a jury trial.[1] Building on the Supreme Court's 2024 Jarkesy decision, the Fifth Circuit struck down a $57 million FCC fine against AT&T (April 2025), and the Supreme Court has agreed to hear FCC v. AT&T to resolve whether FCC monetary penalties violate the Seventh Amendment.

The reasoning extends directly to other agencies that impose monetary penalties through administrative adjudication — including the FCC. If the same principle applies to FCC robocall fines:

- Every FCC fine for robocall violations would require a full federal jury trial
- The DOJ would need to prosecute each case individually, and lacks resources to do so at scale
- The FCC would be left only with the "sledgehammer" of network disconnection (RMD purges) — a binary, all-or-nothing tool that creates disproportionate consequences
- Risk of critical 911 infrastructure outages if regional carriers are disconnected for non-compliance

[1] SEC v. Jarkesy, 603 U.S. ___ (June 2024). Chief Justice Roberts, writing for the majority, held that "when the SEC seeks civil penalties against a defendant for securities fraud, the Seventh Amendment entitles the defendant to a jury trial."

KEY FINDING

The FCC's fine collection rate is already 0.003%. If Jarkesy eliminates administrative fining authority altogether, the FCC loses its primary enforcement tool — leaving only network disconnection, an instrument too extreme for routine compliance failures and too blunt to create graduated deterrence.

8

The Foreign Robocall Elimination Act and Emerging Federal Legislation

Congressional Awareness Is Growing

Congressional awareness of the telecom regulatory gap is growing. The Foreign Robocall Elimination Act and related legislative proposals aim to:

- Require gateway providers (the first U.S. carrier to receive foreign-originated calls) to implement enhanced call authentication and blocking[1]
- Mandate real-time call blocking for traffic originating from known bad-actor foreign carriers
- Extend STIR/SHAKEN requirements to gateway providers that currently operate under exemptions
- Create new reporting obligations for foreign call traffic patterns

These proposals represent a welcome shift toward upstream enforcement. However, they address only one dimension of the problem — foreign-originated calls — while leaving domestic VoIP providers and TDM network bypass vulnerabilities largely unaddressed.

[1] See S. 1509 / H.R. 3150, Foreign Robocall Elimination Act (introduced 2025). The bill targets gateway providers as the critical chokepoint for foreign-originated robocall traffic entering U.S. networks.

9

Closing the Gap: Policy Recommendations

Five Actionable Steps for Upstream Enforcement

9.1 The Clean Framing

Caller ID spoofing is not illegal because the technology exists — it is illegal when used "with intent to defraud, cause harm, or wrongfully obtain anything of value."[1] So if you are serious about prevention, you start where the fraud begins: the spoofed call and impersonation.

The FCC's rules already say providers have to "know their customers" and take "af-

[1] 47 U.S.C. § 227(e)(1).

firmative, effective measures" to prevent customers from using their networks to originate illegal calls[2] — and the FCC has still had to remove and bar large numbers of non-compliant providers from network access through the Robocall Mitigation Database.[3] That is an upstream failure, not a kiosk failure.

9.2 Five Specific Recommendations

1. **Enforce existing telecom KYC rules with financial-sector rigor.** The rules exist.[4] The enforcement does not. The FCC waited until 2025 to bring its first KYC case against a VoIP provider.[5] Apply the same enforcement frequency and penalty severity that FinCEN applies to money transmitters.

2. **Close the TDM network bypass vulnerability.** STIR/SHAKEN is meaningless if scammers can strip digital signatures by routing through legacy copper networks. Mandate carrier-level solutions for authenticating calls that traverse TDM segments.[6]

3. **Create financial liability for careless attestation.** Carriers that grant A-Level trust ratings to scammers should face financial consequences — shared liability for fraud losses, forfeit of surety bonds, or mandatory insurance. Currently, a carrier can stamp the highest trust rating on a fraud call with zero financial exposure.[7]

4. **Mandate Confirmation of Payee at the bank level.** The UK's system **reduced related fraud cases by nearly 60% since its 2020 launch** (European Payments Council), with annual APP fraud declining 17% in 2023.[8] The U.S. has no comparable requirement. This is a proven, bank-stage intervention that addresses the critical gap in wire transfer verification without banning any financial product.

5. **Protect — and strengthen — financial endpoint compliance.** Rather than banning Bitcoin ATMs, mandate industry-wide adoption of the multi-layered fraud prevention measures that leading operators like Byte Federal have implemented voluntarily: trained human BSA officer behavioral review, mandatory scam education, live human intervention for elderly customers, and anti-fraud Terms of Service.[9]

---

[2] 47 C.F.R. § 64.6305(b).

[3] FCC Robocall Mitigation Database enforcement actions (2025), supra notes 13–14.

[4] 47 C.F.R. § 64.6305(b).

[5] See In re Telnyx LLC, FCC File No. EB-TCD-22-00035822, Notice of Apparent Liability for Forfeiture (2025).

[6] FCC, STIR/SHAKEN Implementation: Status and Challenges, Report to Congress (2024) (acknowledging TDM interoperability as the "single largest gap" in the framework).

[7] See TransNexus, STIR/SHAKEN Effectiveness Analysis (2025) (finding that 48% of illegal robocalls carry A-Level attestation).

[8] European Payments Council, Transforming Payment Security: The Journey of Confirmation of Payee in the UK (2024); UK Payment Systems Regulator, Confirmation of Payee: Implementation and Impact Assessment (2024). Note: An earlier Dutch IBAN-name check showed 50% fewer misdirected transfers — a separate implementation from the UK CoP system.

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

9.3 Language That Is Provocative Without Being Sloppy

For policymakers and advocates who need precise, defensible language:[10]

- On the upstream problem: "Caller ID spoofing is not illegal because the technology exists — it is illegal when used 'with intent to defraud, cause harm, or wrongfully obtain anything of value.' If you are serious about prevention, you start where the fraud begins: the spoofed call and impersonation."[11]
- On telecom accountability: "The FCC's rules already say providers have to 'know their customers' and take 'affirmative, effective measures' to prevent illegal calls — and the FCC has still had to remove over 1,200 non-compliant providers from the network. That is an upstream failure, not a kiosk failure."[12]
- On banks: "A $10,000+ cash withdrawal is a CTR-triggering event — reportable, documented, and filed within a defined period. A suspicious transaction at $5,000+ triggers SAR rules, and SARs are confidential. None of that automatically equals 'the bank must deny the withdrawal.'"[13]
- On the real question: "If regulators and advocacy groups truly want to protect seniors, 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?"[14]

[10] All language in this section is sourced directly from the statutes, regulations, and government reports cited throughout this document.
[11] 47 U.S.C. § 227(e)(1).
[12] 47 C.F.R. § 64.6305; FCC enforcement actions, supra notes 13–14.
[13] 31 C.F.R. §§ 1010.311, 1020.320.
[14] 47 C.F.R. § 64.6305 (telecom KYC obligations); CFPB elder exploitation guidance, supra note 42 (bank-stage intervention strategies).

10

Conclusion: Close the Front Door

Enforce Existing Laws at the Source

Every chapter of this report points to the same structural reality: the rules to prevent telecom-enabled elder fraud **already exist**. What does not exist is enforcement proportional to the harm.

The FCC waited until 2025 to bring its first telecom KYC case. STIR/SHAKEN — after hundreds of millions of dollars in industry investment — still grants A-Level trust to nearly half of illegal robocalls. The FCC's fine collection rate rounds to zero. Bank reporting rules document fraud after the fact but do not stop it in progress. And the one proven upstream intervention — Confirmation of Payee — has not been adopted in the United States despite reducing related fraud cases by nearly 60% in the UK since 2020.

Meanwhile, the most heavily regulated participants in the fraud chain — crypto ATM operators who spend $500K–$2M annually on compliance, file SARs, verify identities, and actively intervene to prevent elder fraud — are the ones facing legislative bans and public blame.

The evidence presented in this report leads to one conclusion:

ENFORCE EXISTING LAWS

The rules to prevent telecom-enabled fraud already exist. The enforcement does not. Close the telecom regulatory gap by enforcing existing laws with the same rigor applied to the financial institutions that are blamed for the fraud they did not originate.

Companion documents: The Architecture of Exploitation (fraud architecture analysis) | Securing the Bridge (financial inclusion and unbanked impact)

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

A.2 Federal Regulations

[4] 16 C.F.R. Part 310 (Telemarketing Sales Rule)

[5] 16 C.F.R. Part 461 (Rule on Impersonation of Government and Businesses)

[6] 31 C.F.R. § 1010.306(a)(1) (CTR Filing Deadline)

[7] 31 C.F.R. § 1010.311 (Currency Transaction Report Requirements)

[8] 31 C.F.R. § 1020.320 (Suspicious Activity Report — Banks)

[9] 47 C.F.R. § 64.6305 (Robocall Mitigation and STIR/SHAKEN Requirements)

A.3 Court Cases

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

A.4 FCC Orders, Enforcement Actions & Reports

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

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

[13] FCC, Second Report and Order, WC Docket No. 17-97 (STIR/SHAKEN Framework)

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

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

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

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

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

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

A.5 FTC Rules & Enforcement

[20] FTC, Rule on Impersonation of Government and Businesses, 89 Fed. Reg. 15,072 (Mar. 1, 2024)

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

A.6 Government Reports & Guidance

[22] 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

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

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

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

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

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

A.7 Industry Research

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

A.8 Legislative Proposals

[29] S. 1509 / H.R. 3150, Foreign Robocall Elimination Act (introduced 2025)

A.9 Byte Federal Sources

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