Tackling Financial Fraud: Industry Proactive Efforts and Whole-of-Government Solutions

Paul Benda | Executive Vice President, Risk, Fraud and Cybersecurity | American Bankers Association

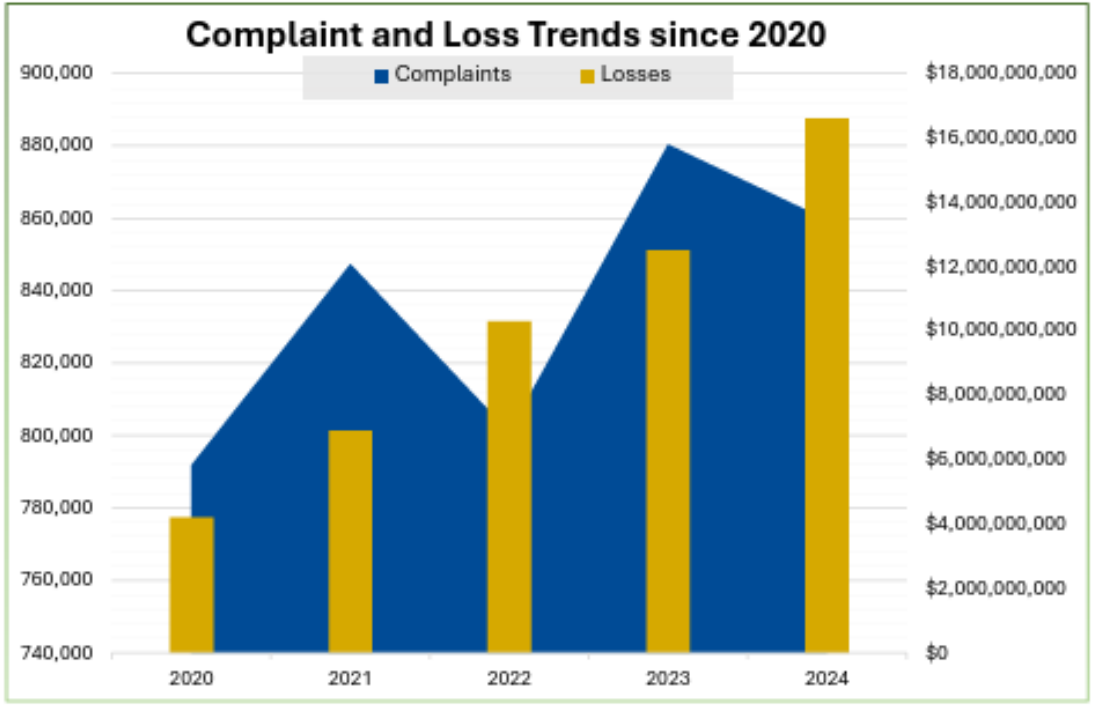
Jason Lane | Senior Vice President, Director of Government Relations | California Bankers Association

Building Success. Together.

Agenda Items

1. Fraud and Scam Trends
2. How are These Scams Enabled - Role of Telecoms and Social Media
3. Crypto ATMs

FBI IC3 – 2024 Internet Crime Report

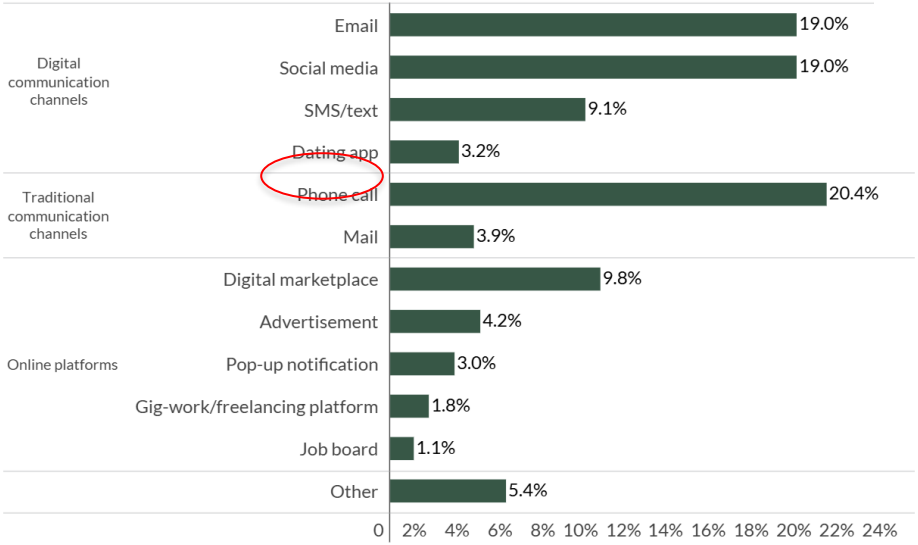


- 2024 – $16.6B in losses
- 33% increase from 2023
- Identity Theft – Rampant in pandemic fueled by Unemployment Insurance fraud – loss of personal data
- 2024 National Public Data Breach – 2.9B personal records

Scams Landscape

Scammers' channels for initial contact

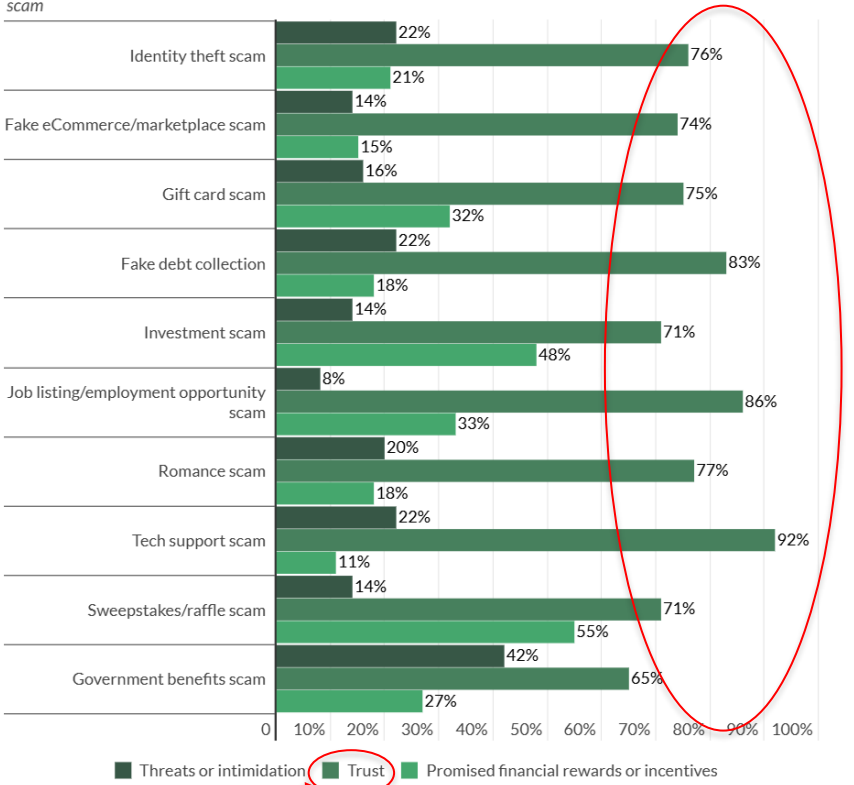
Share of financial scam victims reporting scammers made first contact through select channels



Source: PYMNTS Intelligence
How Scammers Tailor Financial Scams to Individual Consumer Vulnerabilities, January 2025
N = 2,209: Respondents who have experienced household financial loss because of a scam, fielded July 26, 2024 – Aug. 19, 2024

Financial scam compliance tactics

Share of financial scam victims reporting select tactics that scammers used to gain their compliance, by type of scam

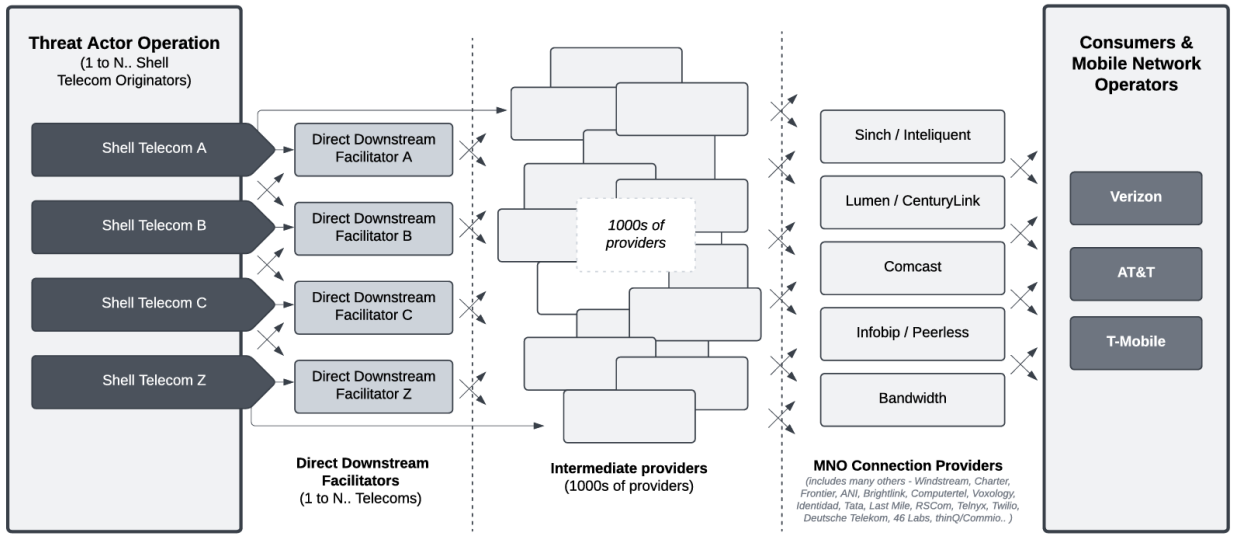


Source: PYMNTS Intelligence
How Scammers Tailor Financial Scams to Individual Consumer Vulnerabilities, January 2025

Stolen personal data used to gain trust

FCC Tracks “Traceback” Requests

- Traceback – identifies telecom enabling reported calls and spoofed caller ID
- Telecom ecosystem very complex



System Vulnerabilities

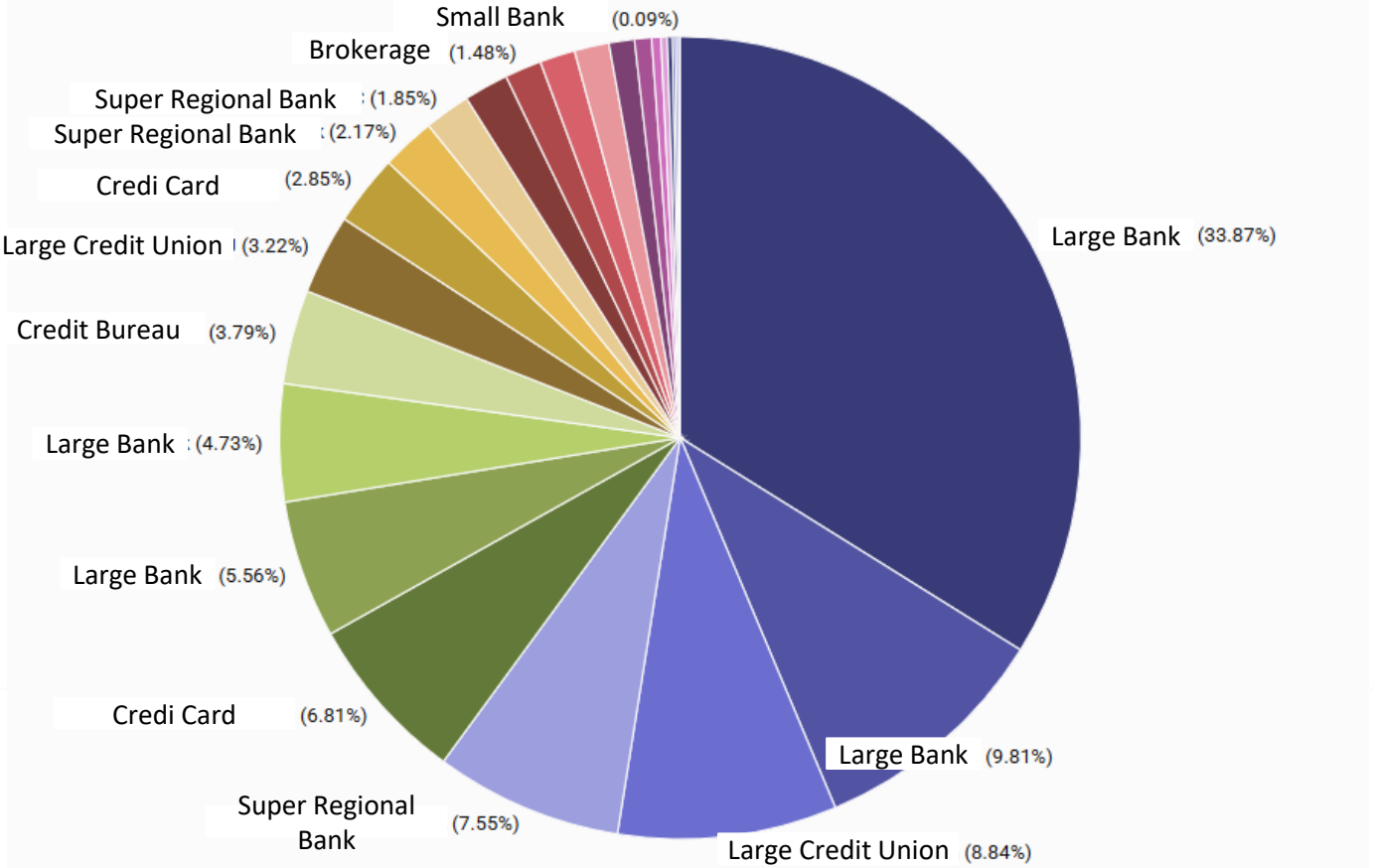
- No KYC on telecom owners - “Shell Telecoms”
- Enables individual bad actors to have dozens
- Feed hundreds of millions of calls into ecosystem
- No accountability

A Study In Toll Free Number Spoofing Of Financials

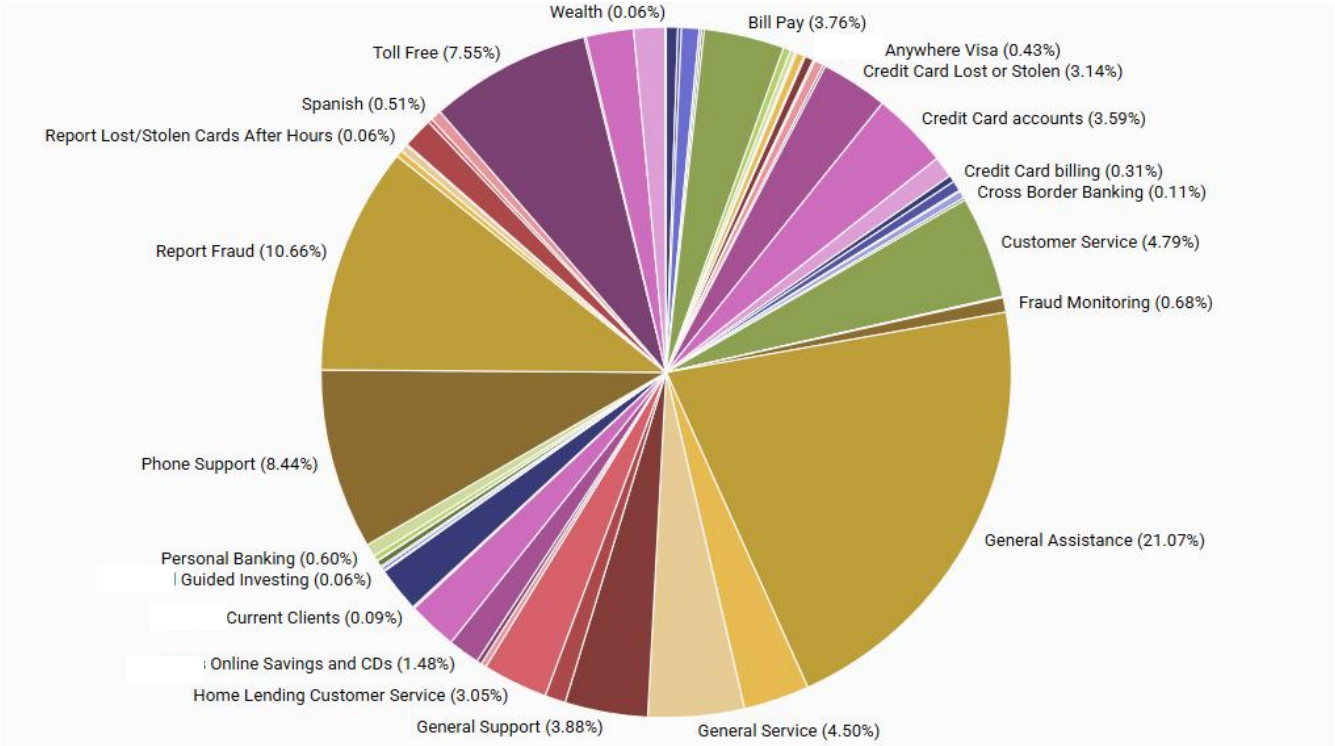
The study involved top banks, credit unions, payment networks:

- Used FCC traceback reporting database to find spoofed calls
- Picked 27 Financial Institutions and identified 118 toll-free numbers owned by them
- Found 7,500 SHAKEN tracebacks where an FI was spoofed
- Analysis of the 7500 calls showed - 237 distinct telecom providers attesting calls

Over half the spoofing afflicted just 3 FIs



Type of Number Spoofed



21% General Assistance

11% Report Fraud

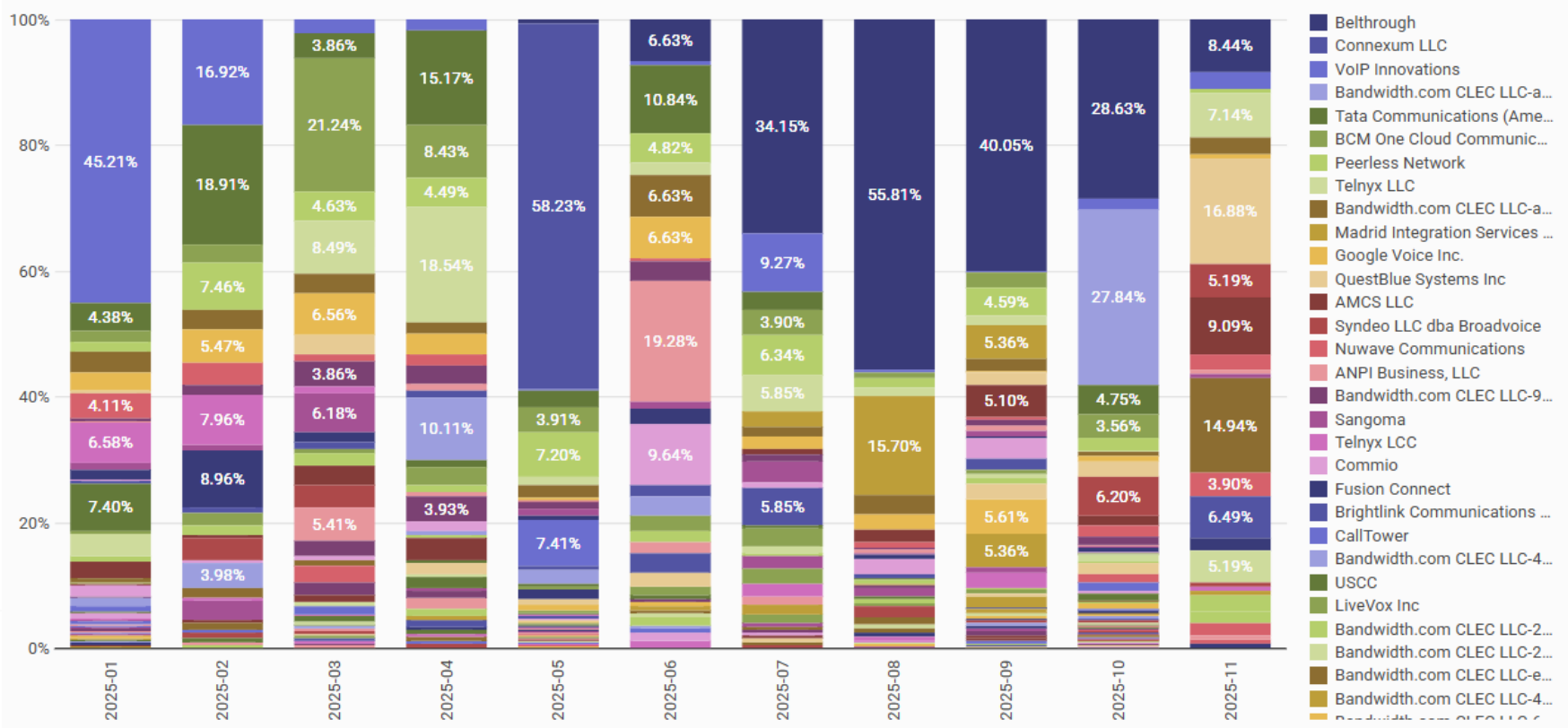
8.4% Phone Support

7.5% General Toll Free

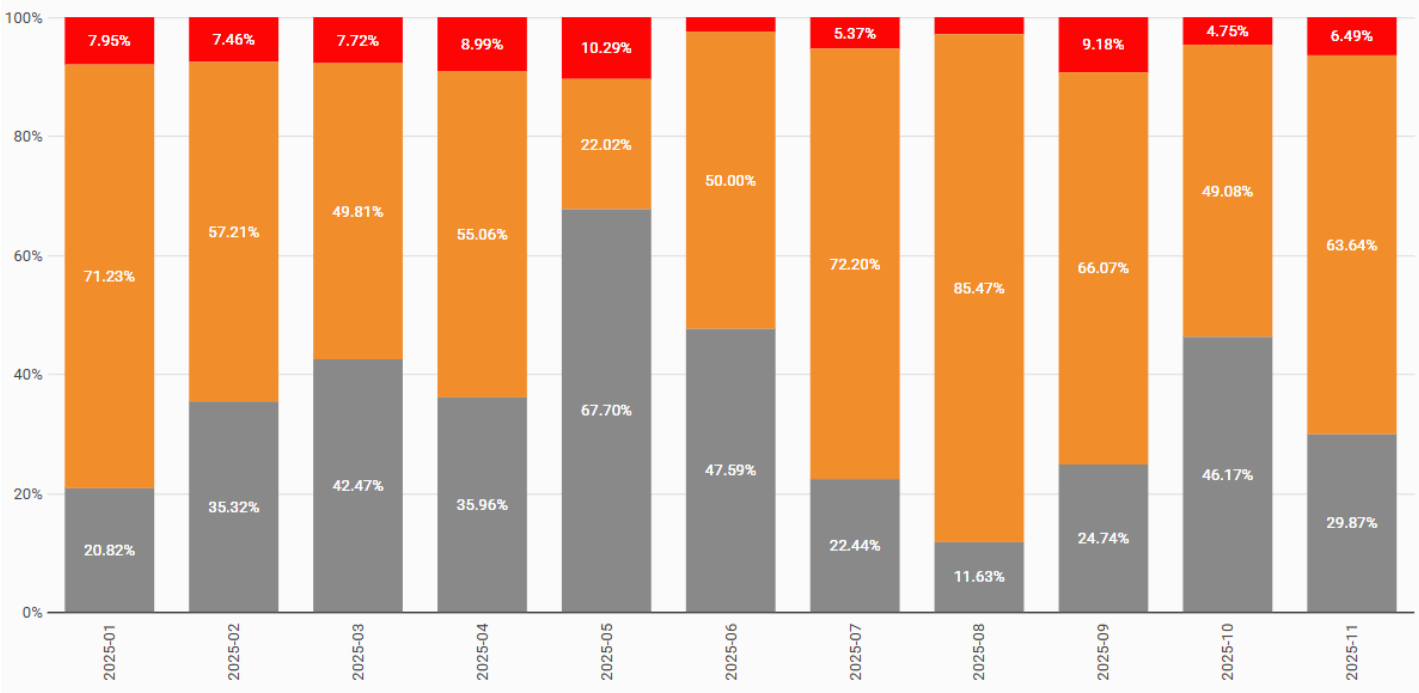
4.8% Customer Service

Spoofing Powered by 237+Providers

Ranked by Percentage of calls hosted



More Than Half of Spoofed Numbers are A or B Attested



A- Level attestation

Provider knows the caller **and** confirms they are **authorized to use the calling number**

B-Level Attestation

Provider knows the caller **but has not verified** they are authorized to use the calling number

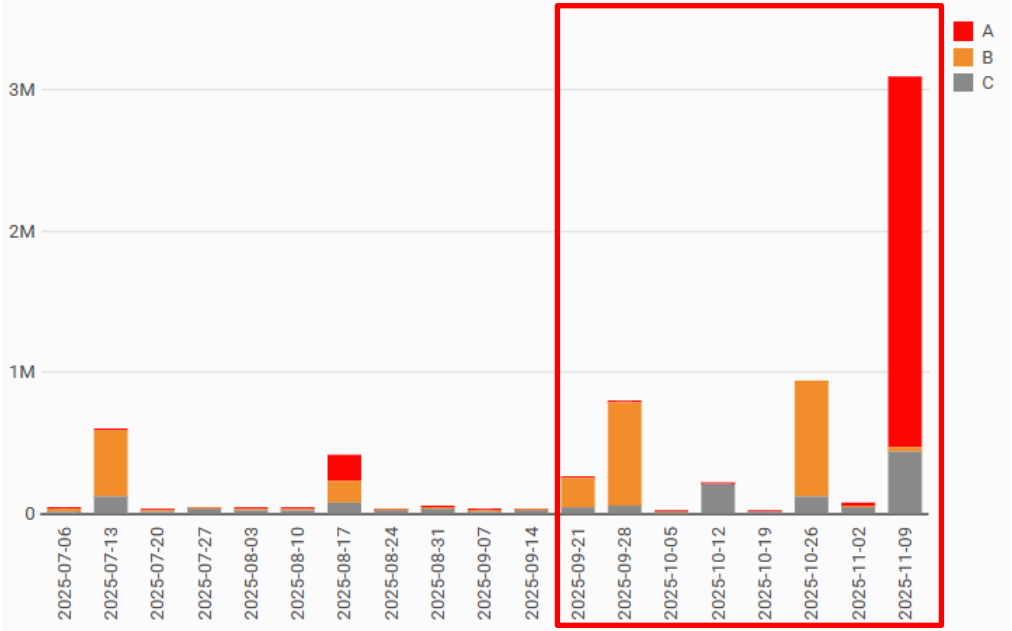
C-Level Attestation

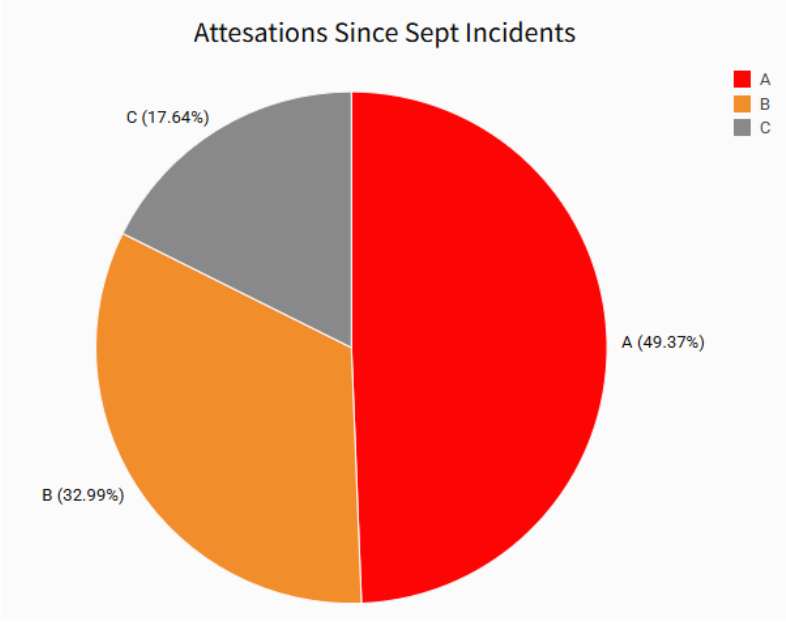
Provider **cannot verify** the caller or their authorization and only knows the call entered its network.

>> A & B attests could be used in Branded Calling as well

Example Recent Attack

Eight week period examined





>> During the incidents, majority of robocalls were A or B attested

(in Nov 9 incident, the C attested calls likely lost A,B they carried)

Top Bank Hit With
10 Million Robocalls in 8 Weeks

> Hello, this is an automated alert from [BANK NAME]. A purchase was declined for $328.99 at [RETAILER/SITE]. Press 5 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) XXX-XXX. To repeat this message, please press 1.

(all incidents use approximately similar messages)

6 incidents.. each over half a million robocalls in just 8 weeks
Largest incident: 4 million robocalls (and counting)
Average incident duration: 3 days - **50% of the calls were A-attested**

Example Transcripts

Week	Example
Nov 9	**5 million robocalls like:** Hello, this is an automated alert from Bank XYZ. A purchase was declined for $328.99 at GameStop.com. Press 5 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 700-0564. To repeat this message, please press 1.
Nov 2	**½ million robocalls like:** Bank XYZ alerts. A purchase was declined for $128.99 at iga.com. Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 221-9093. That is (800) 221-9093. To repeat this message, press any key now.
Oct 26	***1 million robocalls like:*** *This is an automated message from **Bank XYZ** Alerts. We've detected a potentially suspicious transaction on your account. To hear the details of this activity, please press 1. If you would like to end this call now, press the star key. Again, press 1 to review the transaction, or press star to hang up. A purchase was declined for $122 **at Amazon.com.** Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (833) 200-7521.*
Oct 12	**½ million robocalls like:** Bank XYZ, a purchase was declined for $319.55 at Target.com. Press 1 if you recognize this purchase. If you do not recognize this purchase, call our fraud department immediately at (800) 401-5414.
Sept 28	***1 million robocalls like:*** *Hello, this is Automated Message from **Bank XYZ** Telephone Banking. For your security, we monitor your account and have noticed some unusual activity related to your debit card. Please call us back at (844) 587-5633. Once again(844) 587-5633.*
Sept 21	***1.5 million robocalls like: Bank XYZ**, we noticed a recent attempted charge of **$228.15 at Amazon.com**. The transaction was declined for your protection. If you recognize this activity, press 1. If you do not recognize this activity, please call us at (833) 228-1690. I repeat(833) 228-1690.*

Are You More Likely To Answer?

Example of Branded Calling

- New technology being rolled out
- No new technical or telecom originator verifications being proposed
- Very likely see same level of abuse of this new capability as seen with CallerID

>> FCC estimates these calls will be answered 78% of the time

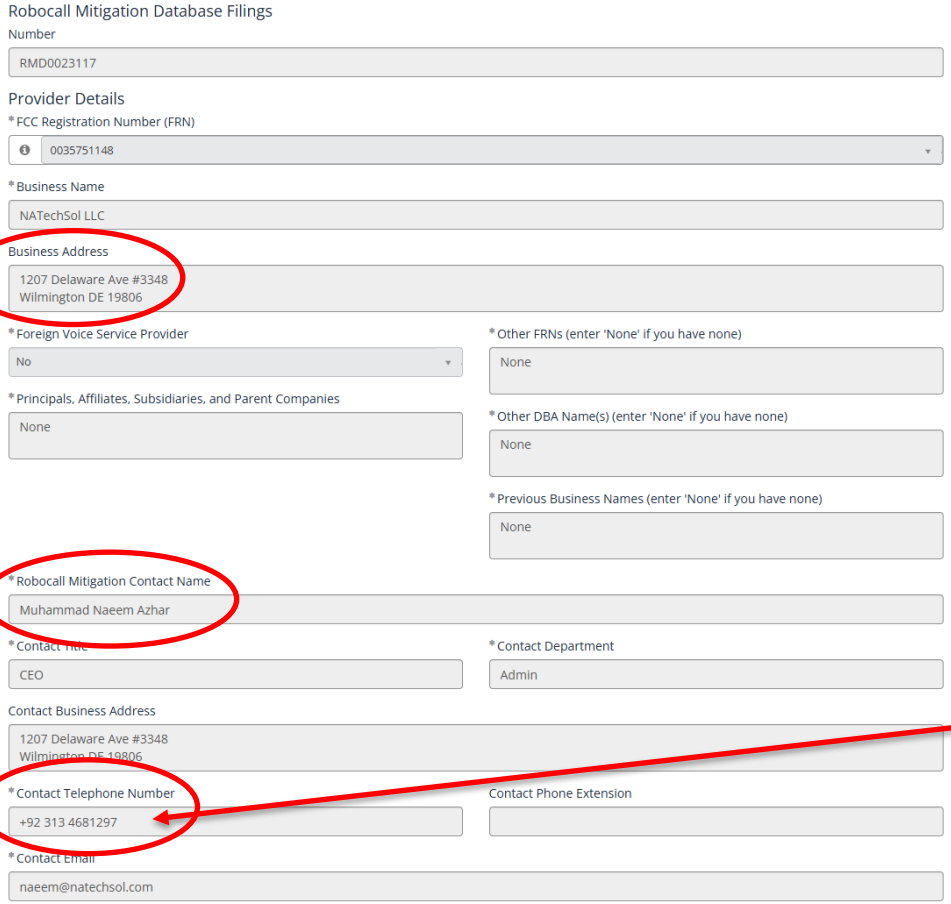
Example of “Bad Actor” Telecom Operations and FCC Registration

Operations : 250M-2.5B Robocalls

Sum of Est Calls		Prd	Robocalls per month					
Org	STI-CA	2025-06	2025-07	2025-08	2025-09	2025-10	2025-11	Grand total
EZ VoIP LLC	Telonium	213,744,000	309,264,000	504,205,000	409,464,000	420,301,000	409,335,000	2,266,313,000
Dial Edge Telecom LLC	Telonium	298,163,000	454,864,000	458,622,000	344,512,000		1,891,000	1,558,052,000
Telcast Networks	Peeringhub	435,817,000	377,849,000	202,215,000	189,851,000	198,031,000	141,993,000	1,545,756,000
ABvoiptel LLC	Telonium	197,012,000	205,715,000	184,398,000	80,664,000	105,178,000	157,976,000	930,943,000
Dial Edge Tel	Peeringhub				120,688,000	345,500,000	317,744,000	783,932,000
Navitech Solutions LLC	Peeringhub			17,886,000	2,590,000			20,476,000
	Telonium	172,513,000	205,135,000	107,430,000	47,429,000	45,009,000	44,346,000	621,862,000
[redacted]veytel	Peeringhub	53,084,000	121,367,000	134,297,000	98,005,000	19,732,000	107,374,000	533,859,000
[redacted]Essential LLC	Telonium	42,804,000	84,413,000	83,682,000	93,840,000	71,537,000	74,540,000	450,816,000
NATECHSOL LLC	Peeringhub			49,745,000	136,589,000	102,259,000	138,175,000	426,768,000
Callsto	Peeringhub			77,195,000	189,157,000	86,899,000	54,265,000	407,516,000
VoyageNetworks	Peeringhub	86,011,000	57,747,000	53,829,000	78,324,000	52,342,000	47,528,000	375,781,000
Telecom Business Network LLC	Peeringhub	83,535,000	63,933,000	47,232,000	92,975,000	80,321,000	4,534,000	372,530,000
Visibi LLC	Peeringhub		428,000	24,768,000	65,290,000	205,974,000	63,007,000	359,467,000
Voipedia	Peeringhub	72,092,000	110,955,000	86,964,000	71,258,000	16,637,000	1,119,000	359,025,000
Fazitel LLC	Telonium				49,603,000	110,051,000	192,834,000	352,488,000

- Legitimate telecoms do not start from zero calls to 50M in a month
- NATECHSOL just one example – others on the screen
- STI-CA is Certificate Authority that grants access to telecom system
- Notice same two CA's on all records

NaTechSol Robocall Mitigation Database (RMD) Filing


Robocall Mitigation Database Filings

Number

RMD0023117

Provider Details

*FCC Registration Number (FRN)

0035751148

*Business Name

NATechSol LLC

Business Address

1207 Delaware Ave #3348
Wilmington DE 19806

*Foreign Voice Service Provider

No

*Other FRNs (enter 'None' if you have none)

None

*Principals, Affiliates, Subsidiaries, and Parent Companies

None

*Other DBA Name(s) (enter 'None' if you have none)

None

*Previous Business Names (enter 'None' if you have none)

None

*Robocall Mitigation Contact Name

Muhammad Naeem Azhar

*Contact Title

CEO

*Contact Department

Admin

Contact Business Address

1207 Delaware Ave #3348
Wilmington DE 19806

*Contact Telephone Number

+92 313 4681297

Contact Phone Extension

*Contact Email

naeem@natechsol.com

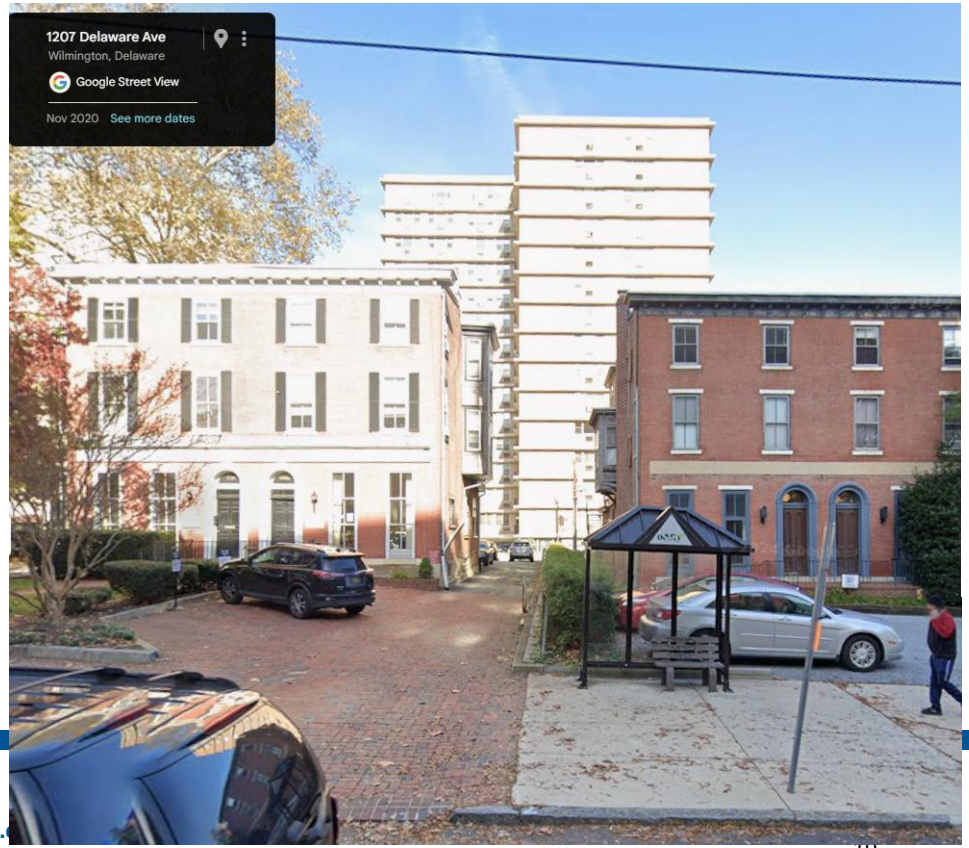
Pakistan Phone Number

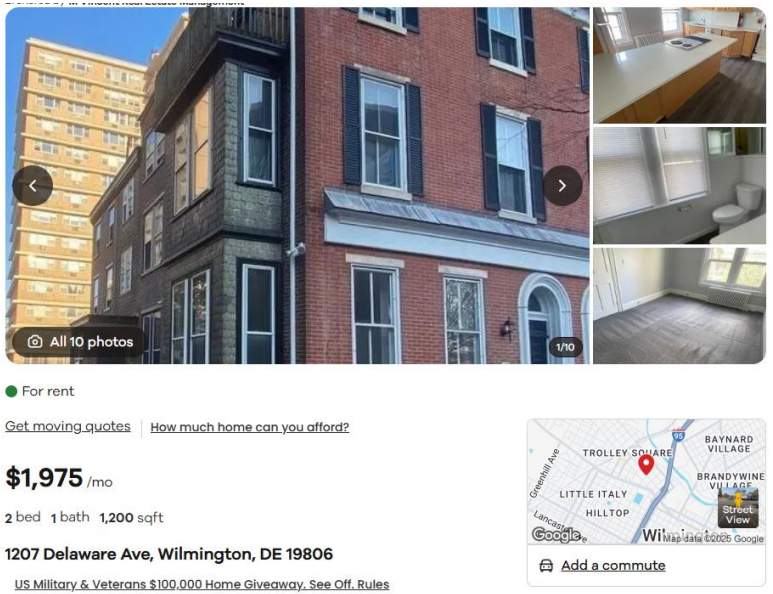
Telecoms Required to Register with RMD

- FCC hosted database
- No checks of information submitted
- No check of required Robocall Mitigation plan
- Some facilitating telecoms don't even check to see if RMD was filed
- Foreign Nationals scamming Americans

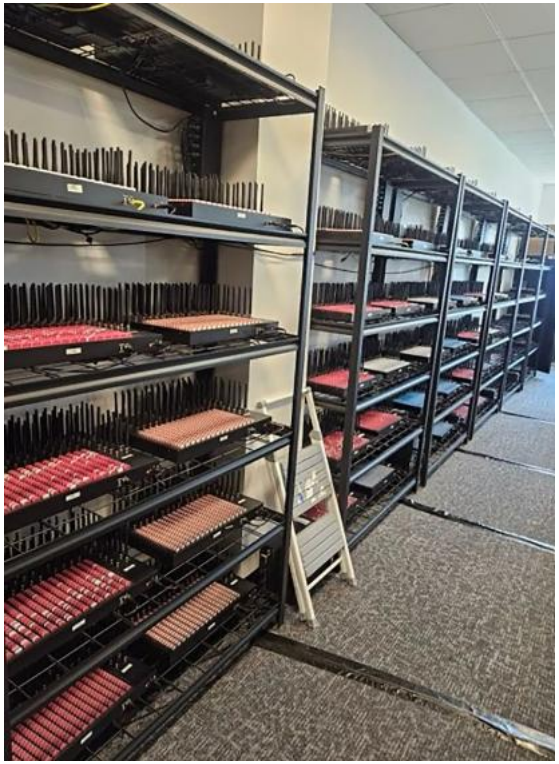
American Bankers Association

NaTechSol – HQ – +400M Robocalls in Four Months





Growth of Pre-paid Sim Card Enabled Scam Calls/Texts



- Recent USSS takedown in NYC
- Sim Farm
  - 100,000 sim cards
  - 300 servers
- mobileX sim cards
  - Use Verizon network
- Likely in operation for nearly a year

https://www.secretservice.gov/newsroom/releases/2025/09/us-secret-service-dismantles-imminent-telecommunications-threat-new-york

https://www.nytimes.com/2025/09/23/us/politics/secret-service-sim-cards-servers-un.html

The Rise of Scams on Meta Platforms*

50%

Scams on Zelle via JPMorgan traced to Meta Ads

8-32

Fraud "strikes" allowed before ad account removal

70%

New advertisers flagged for fraud, illicit goods, or poor-quality offers

230,000+

Scam ads using Andrew Forrest's Name / Image / Likeness

$160B

Meta's ad revenue in 2023 – incentivizing weak enforcement

Section 230 - Meta argues it has no legal duty to protect users from fraud

"Meta has no duty to protect users from third-party content on its platform, Plaintiff cannot state a negligence claim"

*https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8?

Reuters Meta Fraud Article Summary

- Meta projected ~10% of 2024 revenue (~$16B) from scam or banned-good ads
- Users see ~15B scam ads/day plus 22B organic scam attempts.
- Meta only bans advertisers if ≥95% fraud certainty is detected.
- Penalties include charging suspected scammers higher ad auction rates ('penalty bids').
- High-value advertisers can accumulate hundreds of fraud strikes before removal.

https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/

Reuters Meta Fraud Article Summary

- Internal estimate: Meta involved in one-third of successful U.S. scams
- Regulatory pressure rising: SEC probe; UK linked 54% of scam losses to Meta
- Meta ignored ~96% of valid user scam reports in 2023

Rather than voluntarily agreeing to do more to vet advertisers - the company's leadership decided to act only in response to impending regulatory action

Bitcoin / Crypto ATMs

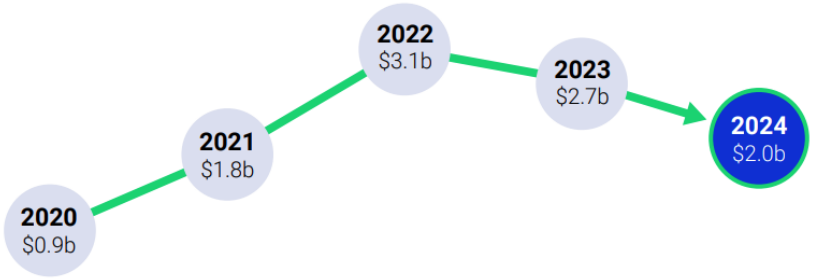
- Crypto Investment Schemes
  - Legitimate looking websites
  - Full functionality
  - “Grow” investment until try to cashout
  - Scammed again with “taxes”

- Bitcoin/Crypto ATMs used to exfiltrate funds
  - Athena sued by DC
  - Fees range 20-30% per transaction
  - 93% of transactions were fraudulent
  - Average age of customer 71
  - Average loss $8,000
- Some states passing BTM laws

International Efforts and State of Scams

- ABA active in International Banking Federation (IBFed)
- ABA Chairs inaugural IBFed Fraud and Scams Taskforce
- Working to ID international best practices across sectors from around the world – establish baseline

Combined losses over last 5 years



Australian Losses

Australia	Canada	Hong Kong	United Kingdom	United States
Improving (losses -26% in 2024)	Slightly worsening (losses+9% in 2024)	Slightly Improving (losses -3.2% in 2024)	Slightly Improving (losses -1.5% in 1H 2024)	Worsening (losses +25% in 2024)
26%	9%	3.2%	1.5%	25%

NASC Report 2024

Australian approach

- The Australian Government proposed mandatory codes on bank, digital platforms and telcos.
- National Anti-Scams Centre (NASC), bringing telcos, banks, law enforcement together to tackle scams at all points of the chain.
- NASC and corporate regulator (ASIC) taking down scam websites (incl fake investments); telcos blocking scam SMS and calls.
- Government introducing a SMS Sender ID Registry to disrupt SMS spoofing.
- Banking industry announcing a voluntary Scam-Safe Accord with industry-wide anti-scam initiatives.

Banks Invest Heavily to Protect Consumers

- Scams and fraud are a huge problem
- Banks do more than any industry to protect their customers but can't do it by themselves
- Tell people don't send money to people you don't know and trust but by the time they're making that payment they believe they know and trust who talking too
- Need to focus on scam prevention
- Shared responsibility
- Telecoms and social media companies are enabling the scammers and profiting from the scam ecosystem

California State Legislation

SB 278 (Dodd)

Expanded the civil definition of “financial abuse” under the Elder Abuse and Dependent Adult Civil Protection Act by:

- Explicitly adding “knowingly aiding or abetting” financial abuse;
- Defining “assists” to include failures by mandated reporters to act reasonably when executing or processing transactions;
- Importing FinCEN red flags into the statutory standard of care; and
- Codifying a negligence-based “knew or should have known” standard for assistance liability

SB 278 (Dodd)

- Introduces secondary liability concepts common in tort law
- Allows plaintiffs to plead knowledge + facilitation, even without direct taking
- Expands exposure beyond primary actors

SB 278 (Dodd)

- The bill does not merely define “assists” — it redefines it to include negligent conduct by mandated reporters.
- Assistance now includes:
  - Executing or processing a transaction when:
  - The elder interacts with the mandated reporter; and
  - The reporter fails to act as a reasonable person given:
  - Transaction history
  - Business practices
  - Presence of multiple red flags

SB 278 (Dodd)

- Frontline Employees Become De Facto Gatekeepers
- Tellers and branch staff are judged against:
  - FinCEN advisories
  - Training they “should have taken”
  - Behavioral interpretation of customers

SB 278 (Dodd)

- Every Transaction Is Litigable in Hindsight
- Plaintiffs can plead:
  - Red flags existed
  - Staff should have known
  - Processing = “assistance”

AB 909 (Schiavo)

Establishes a new liability framework for fraudulently induced transactions involving elders and dependent adults:

- Shifts financial loss from criminals to financial institutions
- Significantly expands institutional reimbursement and litigation exposure
- Modeled after UK Authorized Push Payment Reimbursement Model

AB 909 (Schiavo)

Policy Intent

- Reduce financial harm from scams targeting seniors
- Guarantee reimbursement to victims of fraud
- Position financial institutions as the primary fraud-loss bearer
- Expand enforcement mechanisms and private rights of action
- Introduces concept of “induced fraud”

AB 909 (Schiavo)

Consumer Liability Limits:

- Consumer liability capped at the lesser of $50 or the amount taken before notice of fraud
- Liability may increase if fraud is not reported within 60 days of a statement
- Financial institution bears the burden of proving a transaction was not fraudulently induced

AB 909 (Schiavo)

Investigation & Reimbursement Duties

- Institutions must investigate fraud claims within 10 business days
- Provisional recrediting permitted during investigation
- Consumers retain access to provisionally credited funds while investigation is pending

AB 909 (Schiavo)

Institutional Liability Exposure

- Mandatory reimbursement for fraudulently induced transactions
- Joint and several liability for institutions that receive fraud proceeds
- Limited defenses once a consumer is deemed an injured consumer

Mandated Reporter Expansion

- Expands elder financial abuse reporting duties for bank employees
- Civil penalties up to $10,000 for non-willful violations
- Penalties up to $50,000 for willful violations

AB 909 (Schiavo)

Key Policy Concerns

- Shifts fraud losses away from perpetrators and onto banks
- Encourages defensive banking and transaction denials
- Relies on vague standards subject to hindsight review
- Raises federal preemption and regulatory conflict concerns

CBA Approach

Upstream Solutions

- Consumer education and scam-awareness campaigns
- Scam-disruption at the source (telecom blocking, platform takedowns)
- Law-enforcement coordination and pattern detection (IC3 reporting)
- Federal and state action against organized fraud rings
- Improved authentication standards across payment platforms

Little Hoover Commission Study

In this study the Commission will assess the resources the state currently employs to detect, prevent, and disrupt these scams. The Commission also will examine models at the local level, as well as in other states and counties for opportunities to bolster this work.