

Operation Angels

The Fraud Epidemic

National Emergency

In 2024, the National Public Data breach exposed nearly **2.9 billion records**, underscoring that fraud threatens **all Americans**.

Criminals **impersonate banks** via **fake calls, texts, and emails**, pairing psychological manipulation and social engineering with **spoofed IDs, social media impersonation, and stolen data**.

Even as banks invest millions in chip cards, AI fraud detection, and multi-factor authentication, **scammers keep adapting, threatening consumers and the economy**.

Economic Impact

\$196 billion consumer fraud losses in 2024

25% increase from 2023 to 2024

38% of victims reported losing money

Investment scams claimed the most losses

Imposter scams were second

Collaborative Solution

To combat fraud, an **all-of-government** and **whole-of-ecosystem** approach is essential—bringing together Congress, regulators, telecom, social media, tech, and banks to **protect consumers and reduce scams**.

Banks Protect Their Customers



Banks

- Banks **lead** the private sector in **fraud prevention** but cannot win **the fight against scams** alone
- Consumer education helps, but **scammers exploit trust** with sophisticated tools and tactics
- **Telecoms** and **social media** companies are **enabling scammers** and **profiting from the scam ecosystem**, preventing scams requires cross-sector collaboration and shared responsibility

2025 ABA/Morning Consult Survey



ABA's Fraud-Fighting Campaigns

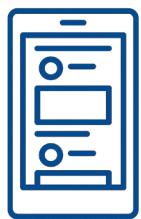
ABA's award-winning [#BanksNeverAskThat](#) and [#PracticeSafeChecks](#) campaigns provide banks of all sizes with turnkey resources to educate consumers and businesses on recognizing fraud and common scams. Participation is free, and more than 2,500 banks have used one or both programs.



Share Responsibility to Protect Americans

Telecoms

- Lack of ownership verification enables “**shell telecoms**” to generate **millions of spoofed calls**
- **Bad actors** can exploit weak controls to push **branded calls** that consumers answer nearly **80%** of the time
- Without accountability, **billions of fraudulent calls** enter the ecosystem unchecked



Social Media

- Nearly **50%** of scams on Zelle for one large bank were traced to **Meta** according to the *Wall Street Journal*, with **70%** of new Meta advertisers flagged for fraud, illicit goods, or poor-quality offers and **96%** of valid user scam reports ignored according to *Reuters*.
- According to *Reuters*, users see **15 billion scam ads** and **22 billion organic scam attempts** daily with Meta earning **\$16 billion—10% of its 2024 revenue**—from scam or banned-good ads, and its platforms linked to **1/3** of successful scams in the U.S.
- *Reuters* also reported that Meta only bans advertisers if **≥95%** fraud certainty is detected with top advertisers accumulating **hundreds of fraud strikes** before removal, and penalties often resulting in Meta **charging bad actors higher rates**.

Fraud Policy Advocacy Framework



State Advocacy

- Support state-level efforts via State Association Alliance to develop clear and consistent fraud-related regulations across all industries
 - **Mississippi Senate Bill 2693** and **Nebraska Legislative Bill 1118** with more states to follow
- Require all telecommunications and social media companies to block fake caller IDs and fake bank text messages, and takedown impersonation accounts
 - **14 states with pending bills addressing caller ID spoofing**



Federal Advocacy

- Establish a White House Office of Fraud and Scam Prevention
- Fix the broken telecom authentication ecosystem
- Bolster state and local support
- Ensure social media platforms protect consumers
 - **Support the bipartisan Safeguarding Consumers from Advertising Misconduct Act**, or the SCAM Act, introduced by Senators Ruben Gallego and Bernie Moreno



International Advocacy

- Work through the International Banking Federation to support G20-aligned efforts