SOMOS®

JANUARY 2026 REPORT

The Cost of Trust:

The Impact of Fraud on Financial Institutions

And the steps toward a more trustworthy future



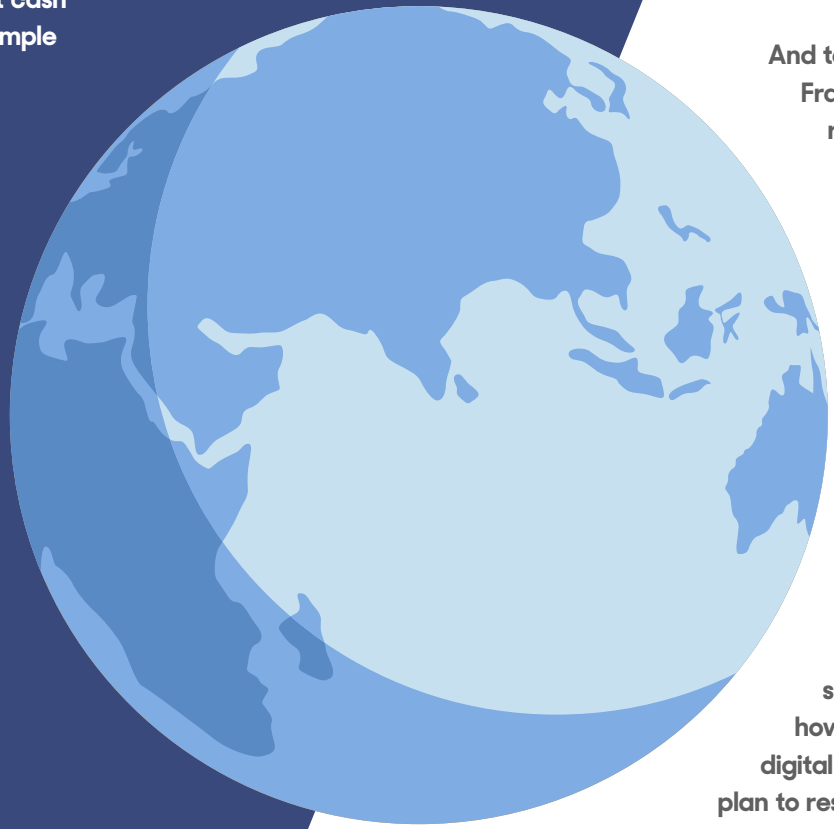
Fraudsters VS Institutions

INTRODUCTION

Financial institutions are no longer just physical places to deposit checks or store savings. They've become a fast-moving, globally connected ecosystem that powers modern life. Markets shift in microseconds through high-frequency trading. ATMs anywhere on the planet enable instant cash withdrawals. Cryptocurrencies are mainstream. A simple photo deposits a check. Today's financial network is faster and more digitally complex than ever.

Layered on top are advanced security tools like multi-factor authentication, behavioral biometrics and blockchain. These technologies highlight both the speed and fragility of the system.

With new capabilities come new risks. The same tools that make finance more secure also create openings for cybercriminals. Sophisticated scams, from phishing and smishing to spoofing, impersonation and payment fraud, target the very systems built to protect us.



And too often, they're successful. Fraud is rising, bringing lost revenue, reputational harm, regulatory pressure and a growing erosion of trust.

Fraud is now a constant threat. Financial institutions need fresh defenses, from advanced detection and real-time monitoring to expert partners. The fight against fraud is escalating, with billions of people's financial well-being at stake.

In this commissioned national survey, we aim to understand how institutions are dealing with digital fraud today and how they plan to respond next.

SOMOS®



The Setup

Somos partnered with Hanover Research to survey over 200 US-based finance professionals. All were 18 or older, worked in banking, credit unions or fintech consulting and held manager-level or higher roles in areas like fraud, IT, risk or digital. Each was familiar with their institution's fraud prevention efforts.



The Focus

The survey focused on telecom and phone-based fraud, its spread, common types and impact on finances and reputation over the past three years. We looked at how institutions are preventing fraud, supporting affected customers and staying compliant with regulations.



The Takeaways

We also explored future priorities like planned investments, new technologies and outside partnerships. The findings show fraud is widespread, costly and damaging to trust. But they also highlight where progress is happening and where more work is needed.

The Rise of Fraud & its Various Forms

Fraud is a universal problem for financial institutions, and it seems to be getting worse.

91%

of respondents reported an increase in the number of fraud attempts over the past year.



According to our results, the single most common fraud vector is phishing, with 98% of institutions having experienced it. These email-based attacks trick recipients into clicking malicious links or sharing credentials, and their realism makes it difficult for customers to trust even legitimate messages.

Close behind phishing are a range of targeted digital and voice-based attacks that exploit consumer trust and FI communication channels.

76%

of institutions reported smishing, or phishing via text.

These scams create a false sense of urgency and familiarity to prompt action, such as clicking a fake link about "suspicious activity."

40%

of institutions are affected by vishing, which targets customers through voice calls rather than text.

This method typically uses spoofed caller IDs, fake emergencies, and pressure tactics to manipulate victims into revealing sensitive information.

39%

of institutions report struggles with robocalls, which flood customers with fake automated messages that mimic legitimate outreach and drown out real communication.

55%

of institutions are impacted by spoofing, which falsifies caller ID information.

45%

of institutions are affected by impersonation where attackers pose as bank representatives.

Both tactics directly erode customer confidence and brand reputation.

75%
Payment Scams

32%
Account Takeover

18%
Interactive Voice Response Fraud

SOMOS®

A Growing Bill

Every organization surveyed reported losing revenue to fraud.

99%
(almost all)

of organizations surveyed experienced a loss of up to 5%of their annual revenue.

But losses aren't the only fraud-related money drain.

As fraud has risen, so have the costs of mitigating it through security and regulatory compliance.

4/5

institutions (80%) said their security costs have increased due to fraud, and 60% have faced higher compliance costs as well.

Regulatory requirements are significant, yet necessary. They demand adapting to constant changes and meeting heightened scrutiny and audit demands – all of which adds up.

Together, the growing need for sophisticated fraud prevention systems and the burden of regulatory compliance are creating a sustained financial strain that extends well beyond the immediate losses from fraud itself.



SOMOS®

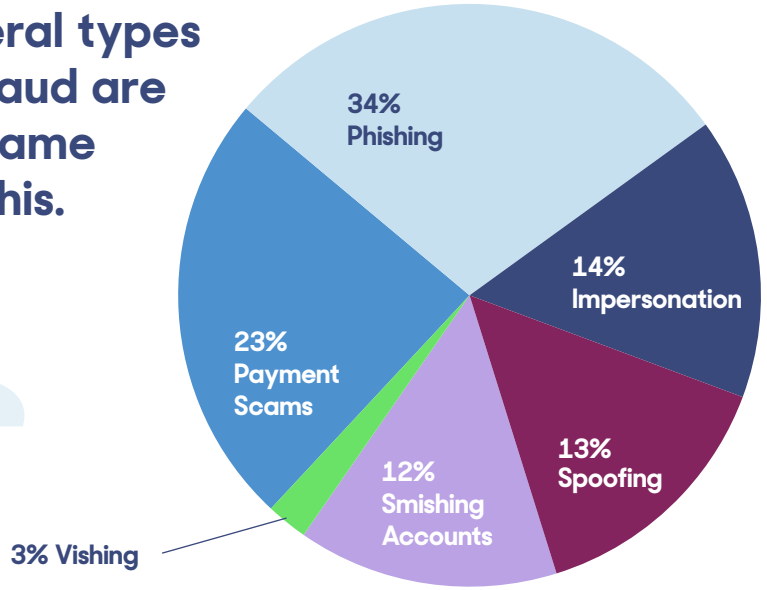
More than Money

As heavy as all of this is, the impacts of fraud on the financial industry go beyond what's accountable in a spreadsheet. They also cause harm to any financial institution's most valuable asset: the trust of its customers.

In other words, the bottom line isn't all that's at stake.

53% of financial institutions said fraud has damaged customer trust.

Several types of fraud are to blame for this.



Together, these are all incredibly caustic to the trust that people need to feel in the organizations that handle their life savings. And once trust is gone, it's incredibly hard to win back.



TRUST

What's Being Done?

On an optimistic note, the industry doesn't seem to be taking any of this lying down. All respondents said they plan to increase spending on fraud prevention in the next three years, and nearly all (99%) consider it a top priority – on par with regulatory compliance and upgrading legacy systems. Technology integration is seen as critical, with more than half planning to make it "much more important" in their strategy going forward.

These planned investments include:

76%
working with external fraud prevention experts

68%
implementing advanced fraud detection technologies

54%
enhancing customer verification and authentication processes

71%
are very likely to add real-time call authentication

70%
advanced fraud detection tools

Regulatory Influence:

Industry regulation is also affecting the way financial institutions are confronting fraud. Just over half of institutions say regulations are pushing them to promote transparency, accountability and continuous monitoring and reporting.

49% enforcing stricter customer authentication

48% requiring adherence to industry standards

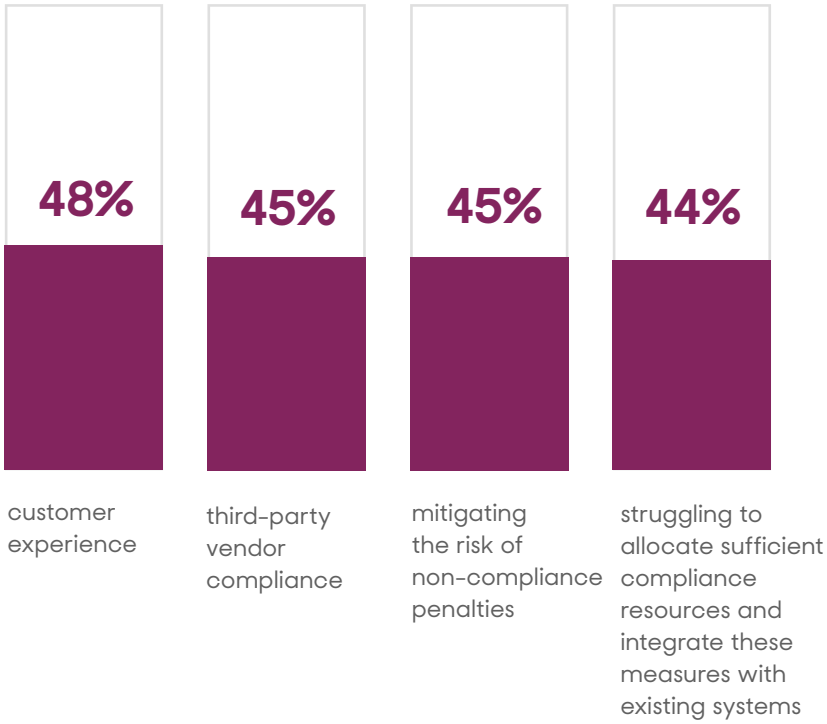
46% mandating regular compliance audits

For around 45% of financial institutions, compliance obligations are also driving bigger investments in telecom security and the implementation of advanced security measures.

But while regulation strengthens fraud defenses, it also introduces new challenges.

58% **of financial institutions report significant hurdles in keeping up with constantly changing requirements and handling increased scrutiny and audits.**

Nearly half of institutions also struggle with balancing fraud prevention



Taken together, the findings tell a two-sided story. While regulatory measures are essential, they're also demanding – pushing financial institutions to adopt stronger protections and stretch their operational capacity.

SOMOS®





Telecom Assets:

Financial Institutions are strengthening fraud defenses by focusing on telecom assets, where many attacks begin.

Nearly all respondents (99%) say upgrading legacy systems is a priority, with 54% calling it a major investment.

Almost as many (96%) are integrating IoT and smart tech to improve connectivity and automation.

Regulatory compliance is also key. About 95% of institutions prioritize it, and 55% consider it a major focus, showing how much regulations shape fraud strategies.

Other priorities include optimizing network infrastructure (88%), managing phone number lifecycles (80%) and tracking telecom assets (78%).

SOMOS®

Partnering With the Pros

Nearly all institutions (95%) are already partnering with specialized fraud prevention providers, and the remaining 5% are at least considering it. Almost everyone seems to recognize how vital these partnerships are, as 98% of participants who partner say it is an important part of their fraud prevention strategy.

Partnerships deliver tangible benefits:

59% access to advanced technology

52% real-time monitoring and alerts

47% improved detection accuracy

Common focus areas include end-to-end call authentication (60%) and live fraud monitoring (60%).



SOMOS®

The Tools

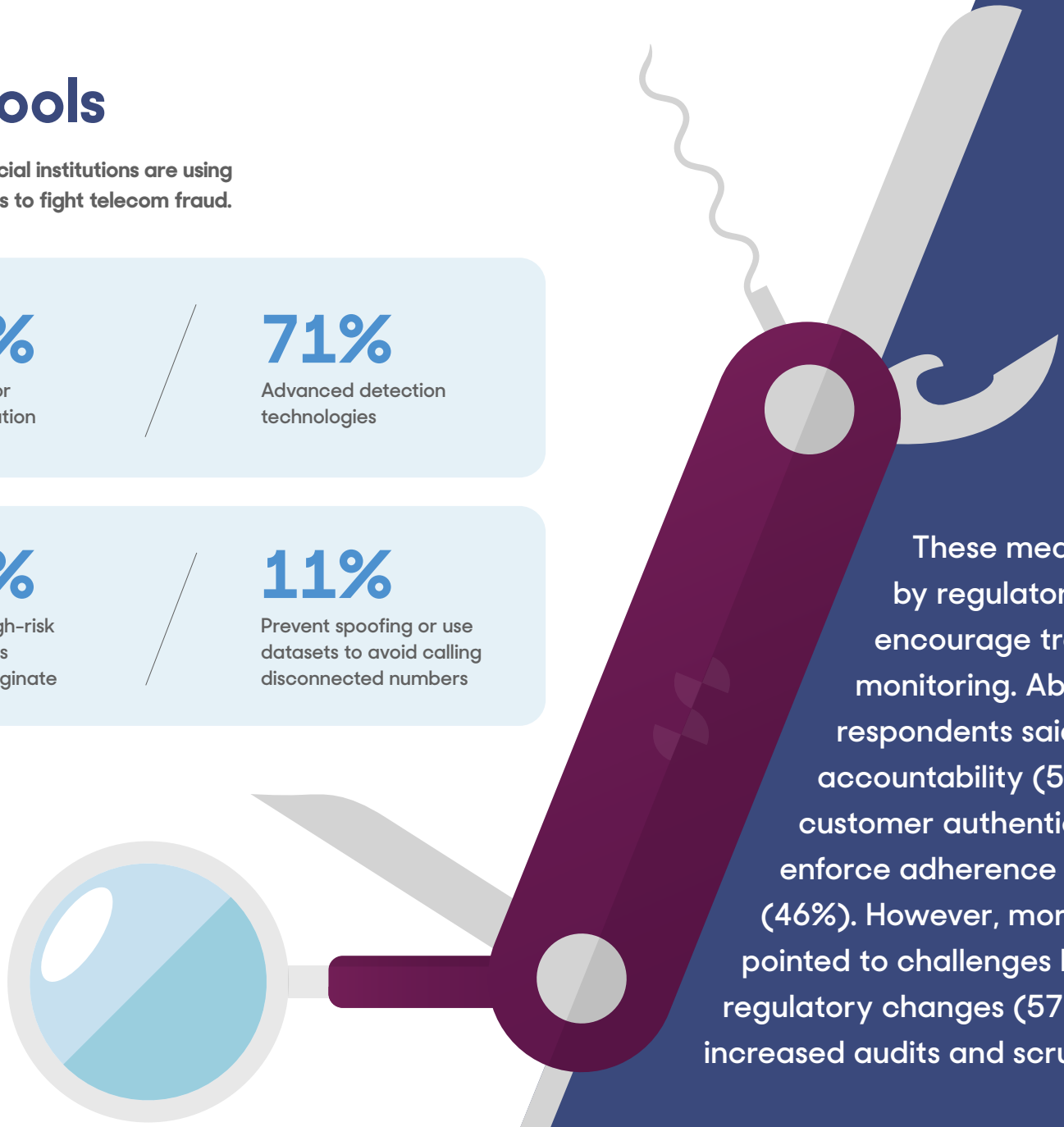
Currently, financial institutions are using a variety of tools to fight telecom fraud.

76%
Multi-factor authentication

71%
Advanced detection technologies

41%
Identify high-risk numbers as Do Not Originate

11%
Prevent spoofing or use datasets to avoid calling disconnected numbers



These measures are supported by regulatory frameworks that encourage transparency and monitoring. About half of respondents said regulations promote accountability (51%), require stricter customer authentication (49%), and enforce adherence to industry standards (46%). However, more than half also pointed to challenges like frequent regulatory changes (57%) and the strain of increased audits and scrutiny (57%).

SOMOS®

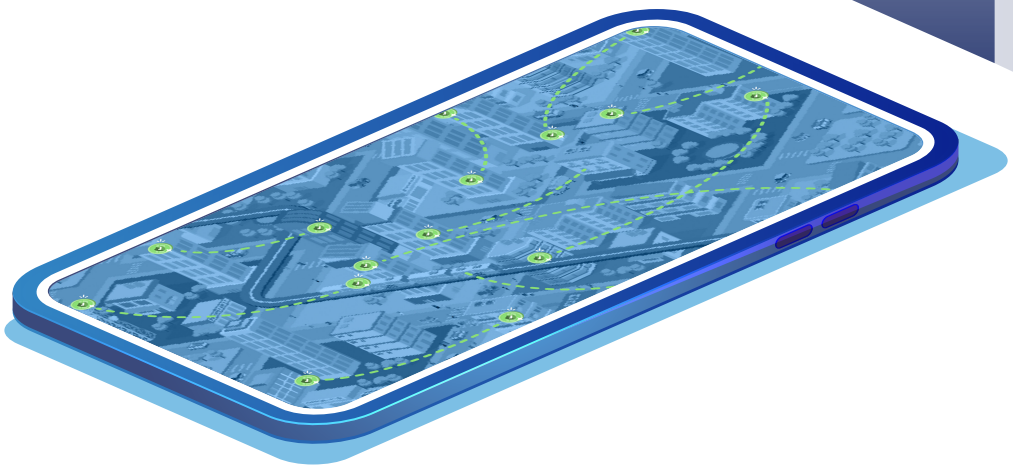
The Gaps that Remain

Even with this level of anti-fraud activity, several results indicate some level of institutional cognitive dissonance on the part of the industry.

93% of financial institutions agree real-time call authentication is important for mitigating fraud risks,

71% yet three-quarters say it makes up less than 25% of their fraud prevention strategy.

Similarly, two-thirds of respondents say they can track fraud losses by phone number, but those capabilities are limited. And while most institutions feel very or extremely prepared to handle fraud (80%), more than six in ten describe their current strategy as only "somewhat proactive" and in need of improvement.



SOMOS®

Spotlight: Somos' Trust Framework for Phone Number Right to Use — Building Trust into Every Call.

The fraud we see playing out in the financial industry is not unique to it. It's an ecosystem-wide problem, and calls for a root-level solution that has yet to exist. That's why Somos is proposing the Trust Framework for Phone Number Right to Use — a series of industry standards to secure the call path from end-to-end, and stop many of these fraud attempts from ever getting off the ground.

From Reactive to Proactive

For years, the telecom industry has fought fraud by trying to block bad actors once they're already in play. And while tools like STIR/SHAKEN and network attestation have been major steps forward, they're ultimately defensive measures which don't tackle fraud at the source. The Trust Framework for Phone Number Right to Use changes that. Instead of chasing intruders already inside, it locks the door, embedding verified identity directly into the call and message path from the start.

How It Works

Before an entity can use a phone number, it must be vetted through Know Your Customer (KYC) or Know Your Business (KYB) checks. These confirm the legal name, address and authority to use the number. Once verified, the entity receives a digital credential which cryptographically tied to the number. This means it proves Right to Use without revealing private data. This proof is recorded in a tamper-evident transparency log, creating an open record that carriers, regulators and partners can check in real time.

Trust from End to End

Every call or message can now be validated all the way along the call path. Carriers can confirm Right to Use easily and legitimate callers can present themselves in a way that earns trust from customers. Fraudsters, unable to get verified credentials, are denied entry before they reach a consumer's screen. The result: Calls and texts become a premium channel of connections between consumers and brands.

How Somos Can Help

The survey results make it clear: Financial institutions face a persistent and evolving fraud challenge that impacts revenue, compliance costs and — most importantly — customer trust. Taking a stand against this threat will mean much more than blocking bad actors. It will mean giving legitimate brands the tools to represent themselves in a clear, verifiable way, so customers can connect with confidence.

As the trusted administrator of several key numbering registries, Somos manages over 7 billion phone numbers as well as the digital identities behind them. Our mission is to ensure that every financial institution can protect its brand and present itself with verified, trusted identity across the call and text channels.

Central to this mission is the authentication of Right-to-Use (RTU) along the entire call path — in other words, confirming that the entity using a number is the one who's authorized to do so. By building this verification into every step of a call or message's journey, Somos helps eliminate the uncertainty and doubt that fraud has so effectively spread.

Email us at
connect@somos.com
to learn more

SOMOS®

Our suite of fraud prevention and identity assurance solutions works directly to address the concerns raised by fraud:

RealBrand®

Centralized management of your phone number assets, with monitoring to detect spoofing, prevent impersonation and fix misleading call labels.

RealAgent®

Verify consumer identity by leveraging phone number intelligence to ensure every interaction is trusted, accurate and fraud-free.

RealNumber® DNO

Blocks calls from "Do Not Originate" numbers that are often exploited for scams.

Together with the Trust Framework — our proposed industry standard for securing the call path — these tools allow financial institutions to implement real-time authentication, maintain visibility into their number usage and meet regulatory expectations for transparency and accountability.

For financial institutions, partnering with Somos means more than saving a few dollars here and there on annual loss reports. It's a chance to reclaiming the integrity of the voice and messaging channels as high-value customer connection points — where every interaction is backed by proven identity and built on trust.