

Telecom Fraud & Community Banks

Protecting Trust Before Fraud Reaches the Transaction

Trust Is a Community Bank's Greatest Asset

Community banks have always operated differently from larger financial institutions. Their strength comes from relationships, local knowledge and a reputation built over years – sometimes generations – of serving customers.

That trust creates loyalty.

It also creates opportunity for fraudsters.

Today, many fraud schemes begin long before a fraudulent transaction appears in a banking system. Criminals increasingly target customers through the communications channels they use every day: phone calls and text messages. By impersonating trusted institutions and exploiting customer confidence, fraudsters manipulate individuals into sharing sensitive information, authorizing payments or compromising accounts.

Community banks and their customers, who expect face-to-face relationships and personal familiarity as a part of doing business, are especially vulnerable to fraudsters willing to capitalize on that trust.

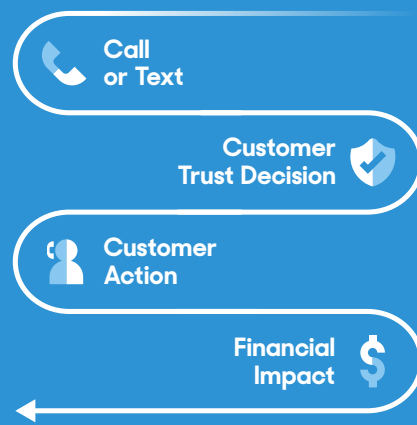
The damage this causes is more than monetary; it strikes at the very relationships that allow these institutions to operate.

That's why these local institutions can no longer view fraud solely through the lens of transactions and account activity. Trust is being attacked earlier in the customer journey.

The New Front Line of Fraud Starts with a Phone Call

Fraud often begins when a customer receives what appears to be a legitimate call or text message from their bank warning of suspicious account activity, or an urgent need to verify credentials, provide a one-time passcode or approve a transaction. These communications often seem authentic because fraudsters have successfully manipulated the phone number, caller ID or messaging information displayed to the customer. As a result, the attack succeeds not because the bank's systems were compromised, but because the customer's trust was exploited.

Fraud Begins with a Trust Decision



The most important moment in many fraud events occurs before a transaction is initiated.

Where Telecom-Enabled Fraud Intersects Banking

Many of today's most common fraud schemes rely on communications channels as the initial point of compromise. And when these communications come from a local institution — one where customers might know their community bankers by name — these schemes can be even more effective.



Bank Impersonation

Fraudsters pose as bank employees, fraud departments or customer service representatives to gain credibility and extract sensitive information.



Caller ID Spoofing

Attackers manipulate caller information to make calls appear legitimate, increasing the likelihood that customers will answer and trust the interaction.



Smishing and Vishing

Text messages and voice calls create urgency around fabricated account issues, security concerns or payment requests.



Account Takeover

Customers are persuaded to share credentials, authentication codes or personal information that allows criminals to gain access to accounts.



Elder Financial Exploitation

Older adults are often targeted through scams that leverage fear, urgency and perceived authority.

The Human Cost

Account Takeover Fraud Is Accelerating

U.S. consumers and businesses lost more than **\$15.6 billion** to account takeover fraud in 2024, as fraudsters increasingly use phishing, spoofed calls, text messages and stolen credentials to gain unauthorized access to accounts.

Source: Federal Reserve Financial Services (2026)



The Phone Number Has Become a Security Signal

For decades, phone numbers were viewed primarily as routing information. Today, they've become something far more important, functioning as trust signals.

Customers use phone numbers to determine whether to answer a call, respond to a text or engage with a message. A familiar number often serves as an indicator of legitimacy.

Fraudsters recognize this behavior and deliberately exploit it.

As a result, telephone number identity is no longer simply a telecommunications issue. It has become an important component of the broader trust ecosystem that supports digital interactions.

Banks have invested heavily in fraud detection, cybersecurity and customer authentication. Yet telecommunication trust often remains outside traditional fraud discussions despite its growing influence on customer decision-making.

Key Insight

A trusted phone number can influence customer behavior before any fraud controls inside the banking environment have an opportunity to intervene.



Bringing Telecom into the Fraud Prevention Conversation

Addressing telecom-enabled fraud requires collaboration beyond any single organization.

Community banks understand customer behavior, transaction patterns and victim support.

Telecommunications organizations understand the infrastructure, numbering systems, authentication frameworks and identity signals that influence trust across communications networks.

Together, these perspectives can create stronger defenses against emerging threats.

Areas where telecom expertise can support financial institutions include:

- Understanding how trusted numbers are represented and protected
- Exploring call authentication capabilities
- Identifying suspicious calling and messaging patterns
- Developing customer education around trusted communications
- Sharing intelligence during emerging fraud campaigns
- Strengthening industry-wide collaboration and awareness

Much of modern financial fraud relies on a lack of cohesion between the banking and telecom ecosystems. By closing that gap through greater collaboration, organizations can eliminate opportunities for scammers to operate.

The Case for a Shared Responsibility Model

Fraud prevention is most effective when organizations share visibility across the customer journey.

Community Banks Contribute:

- Customer relationships
- Transaction intelligence
- Local market awareness
- Fraud response and victim support

Telecom Organizations Contribute:

- Numbering expertise
- Communication identity signals
- Call authentication context
- Registry and routing knowledge

Industry Associations Contribute:

- Education
- Coordination
- Advocacy
- Information sharing

When these stakeholders collaborate, customers receive a more consistent and trustworthy experience.

Looking Ahead: Strengthening Trust Through Collaboration

Trust remains the foundation of every successful banking relationship.

Protecting that trust requires understanding how customers experience communications, how fraudsters exploit those interactions and how organizations can collaborate to strengthen confidence across the entire customer journey.

As the steward of critical numbering infrastructures and telecommunications identity resources, Somos works across the communications ecosystem to help strengthen trust, support industry collaboration and advance conversations about how communications and fraud prevention intersect.

The challenge is shared. The responsibility is shared. And the opportunity to better protect customers begins with bringing banking and telecom leaders together around a common goal: **restoring trust in the world's communications.**

Trust Is Built Across Multiple Systems

Customers do not distinguish between banking infrastructure and communications infrastructure.

They simply decide whether they trust the interaction. That's why fraud prevention must extend beyond transactions and account security to include the communications channels that shape customer decisions every day.



Want learn more about how Somos is **restoring trust in the world's communications?**
Connect with a team member today!

connect@somos.com

