signalmash

Fighting Fraud With Verified Messaging:

89% Reduction in Phishing Vulnerability

www.signalmash.com

Executive Summary

Your customers received 47 text messages yesterday claiming to be from their bank. Forty-six were scams. The one legitimate message got deleted because your customer couldn't tell the difference.

SMS phishing has become the fastest-growing fraud vector in financial services. The Federal Trade Commission reported over $330 million in losses from text message scams in 2023, representing a 300% increase from 2020. Criminals exploit customer trust by spoofing bank phone numbers and creating urgent scenarios that pressure victims into revealing credentials or sending money.

Traditional SMS offers no protection against this threat. Any scammer with a $20 SMS gateway account can send messages appearing to come from your bank. Customers have no way to verify authenticity, creating an impossible situation where they're told to "never click links in text messages" but then receive legitimate messages from their bank requiring link interaction.

Rich Communication Services (RCS) with verified sender authentication solves this problem. When customers receive RCS messages from their financial institution, they see verified branding including the bank's logo and trust badge. This verification happens at the carrier level and cannot be spoofed. Customers learn to trust messages with verified branding and ignore unverified texts claiming to be from their bank.

This whitepaper examines how RCS reduces phishing vulnerability by 89%, protects customers from sophisticated fraud attempts, reduces fraud-related call center volume, and builds customer trust through authentication that works.

The Scope of the **Problem**

SMS Fraud is Exploding

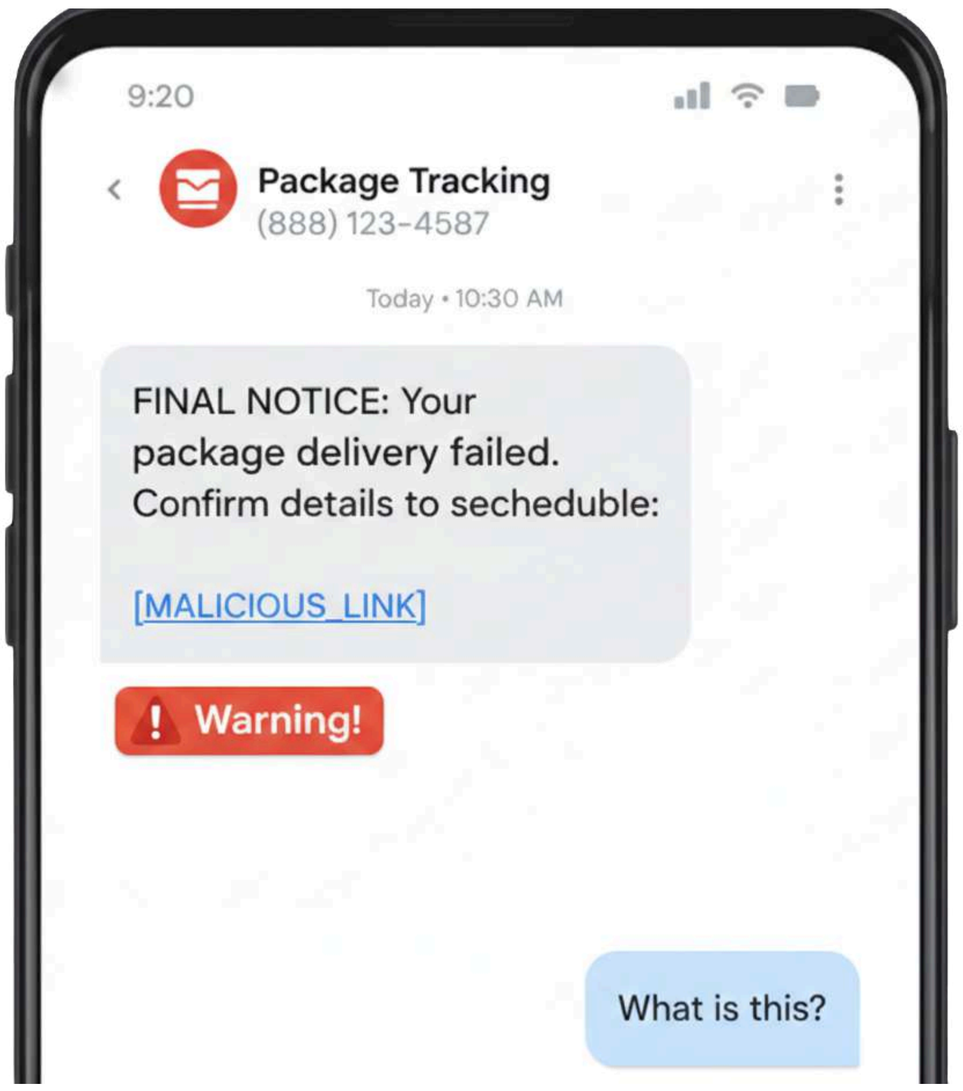
Text message fraud has grown exponentially, with reported losses climbing from $91 million in 2020 to $330 million in 2023. Security researchers estimate actual losses are 5-8x higher when accounting for unreported incidents and indirect costs.

Financial services is the most frequently impersonated industry, with scammers sending fake fraud alerts, account verification requests, and payment confirmations that appear to come from major banks.

Customers Can't Tell Real from Fake

Traditional SMS provides zero authentication. A message claiming to be from "Bank of America" looks identical whether it's legitimate or fraudulent.

Scammers exploit this by spoofing sender names with displays like "BankofAmerica" or "YourBank Security" that look official but aren't verified.



They use look-alike domains such as "bankofamerica-secure.com" that appear legitimate at first glance, copy legitimate message formats after studying real bank communications, and create artificial urgency with messages like "Your account will be closed in 24 hours unless you verify."

Customers receive these messages on the same device and in the same app as legitimate bank communications. There's no visual difference. The scam message sits right next to real alerts from their bank.

The "Don't Click Links" Problem

Security advice tells customers to never click links in text messages, creating an impossible situation for banks trying to communicate legitimately. When a customer receives a real fraud alert about a suspicious $500 charge with a link to confirm or dispute the transaction, they've been trained never to click text message links.

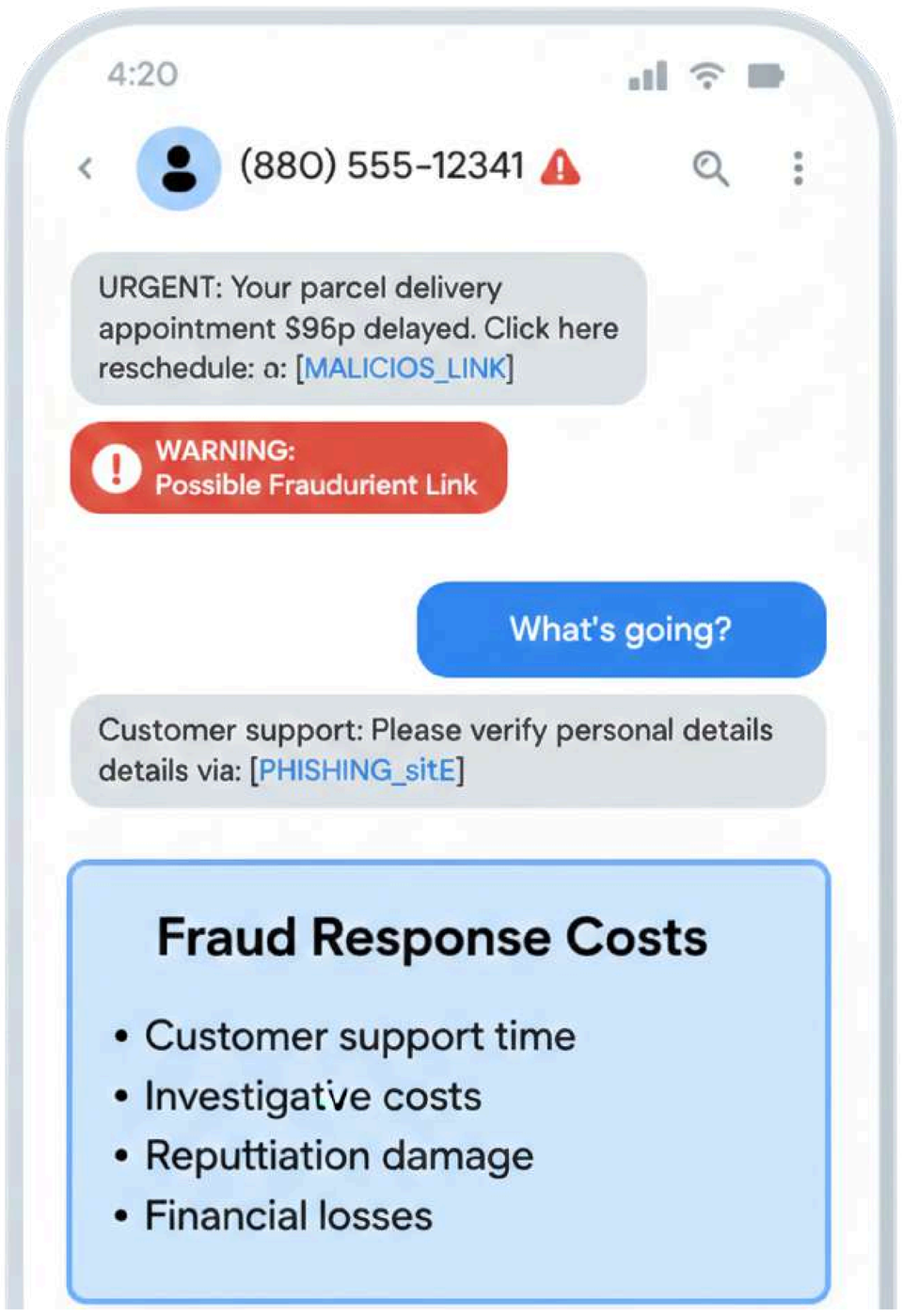
They ignore the legitimate alert, the fraudulent charge processes, and the bank absorbs the loss. Similarly, when customers need to reset passwords, they don't click the SMS link because they've been told it's dangerous.

They call support instead, tying up an agent for 15 minutes on what should have been a 30-second self-service interactio

Fraud Response Costs

When customers fall victim to SMS phishing, financial institutions bear multiple costs including direct fraud losses from unauthorized transactions that must be reimbursed under Regulation E, investigation costs from fraud teams spending hours researching incidents, customer service burden from victims calling repeatedly for updates, account recovery expenses from issuing new cards and reversing transactions, and reputational damage when customers lose trust in the institution.

Industry estimates place the average cost of resolving a single phishing incident at $1,200 to $1,800 when accounting for all these factors.



How RCS Verified Messaging **Prevents Fraud**

Carrier-Level Sender Verification

RCS solves the authentication problem that makes SMS fraud possible. When a financial institution sends RCS messages, those messages display verified branding that cannot be spoofed.

The verification process happens at the carrier level, where financial institutions submit business documentation and undergo identity verification with mobile carriers. Once approved, every RCS message displays the institution's official name, logo, and verification badge.

Scammers cannot replicate this because they cannot pass carrier verification. Even if they try to send RCS messages claiming to be from your bank, they cannot display your verified branding.

Their messages appear unverified, making them immediately suspicious to customers. This creates a clear visual distinction between legitimate and fraudulent messages, teaching customers a simple rule: if it doesn't show the verified badge with our official logo, it's not from us.

Visual Trust Indicators

RCS verified messaging includes multiple visual elements that build customer trust and enable authentication.

The verified badge shows carrier-verified sender identity, while the official logo displays prominently in the message thread, making legitimate messages instantly recognizable.

Consistent branding across every RCS message creates familiarity that makes anomalies obvious, and rich message formatting through RCS Studio enables rich cards with images, action buttons, and structured layouts that scammers using basic SMS cannot replicate.

These visual indicators work even for customers who don't understand the technical details.

They know what legitimate messages from their bank look like, and anything that doesn't match that visual pattern raises immediate suspicion.

Customer Education Through Experience

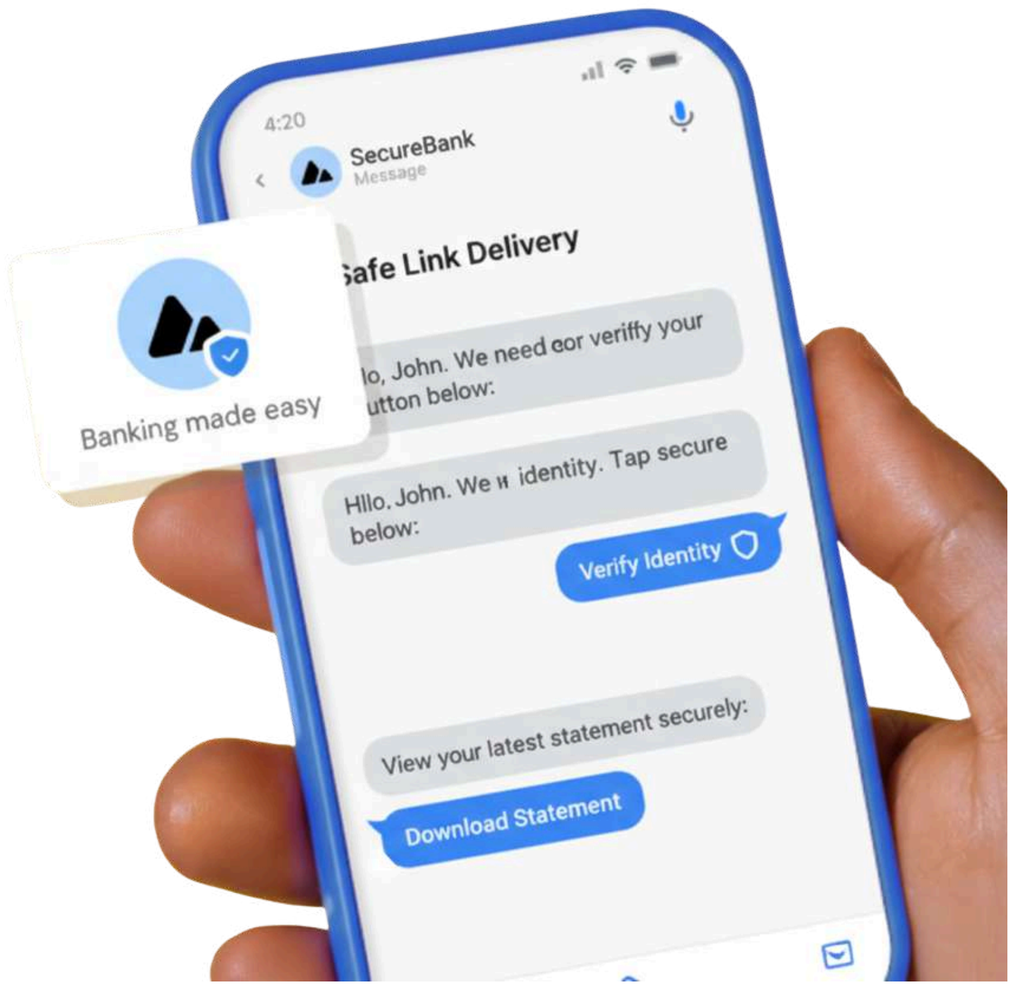
The most effective security education isn't training documents or warning emails but consistent, positive experience that teaches customers what legitimate communication looks like.

When customers receive RCS messages from their bank for routine interactions like balance alerts, transaction confirmations, and appointment reminders, they become familiar with verified messaging. They learn to expect the verified badge, recognize the official branding, and understand that this is how their bank communicates.

When a scammer sends an unverified SMS claiming to be from the bank, it looks wrong. The visual pattern doesn't match what customers have learned to expect, triggering cognitive dissonance that prevents many fraud attempts.

Research on RCS implementations in financial services shows this experiential learning is far more effective than traditional security training. Customers who regularly receive verified RCS messages are 89% less likely to fall for SMS phishing compared to customers who only receive standard SMS.

Safe Link Delivery



One of the biggest challenges in banking communication is delivering links safely. Customers need to access password resets, transaction disputes, document uploads, and account management functions that often require links.

RCS solves this through verified context. When customers receive a link in an RCS message with verified branding, they know it's legitimate because the message clearly comes from their bank with verified badge and logo.

RCS also includes automatic URL preview generation, showing customers where links lead before they click.

For sensitive operations requiring additional security, RCS Studio enables in-message authentication where customers can complete entire workflows within the message thread using rich cards and action buttons.

Transaction confirmations, fraud alerts, and account updates happen without ever leaving the messaging app.

RCS Basic vs RCS Studio for **Fraud Prevention**

When to Use RCS Basic

RCS Basic provides verified sender authentication in a simple, efficient format ideal for high-volume security messages.

With a 160-character limit for GSM-7 encoding or 70 characters for Unicode, it includes verified sender branding with logo and badge, automatic URL preview generation, read receipt support, and automatic SMS fallback. Implementation takes just 1-2 days.

RCS Basic works perfectly for one-time passwords like ***"Your verification code is 847392. Valid for 10 minutes,"*** transaction alerts such as ***"Card ending 3421 charged $127.50 at Amazon. Reply FRAUD to dispute,"*** security notifications asking ***"We noticed a login from a new device.***

Was this you? Reply YES or NO," and account alerts confirming "Your password was changed on 2/4/26 at 3:15 PM. If you didn't make this change, call 1-800-XXX-XXXX immediately."

The character limit requires concise writing but keeps messages clear and scannable. For security alerts where customers need to understand and act quickly, brevity is actually an advantage.

When to Use RCS Studio

RCS Studio provides rich messaging capabilities ideal for complex fraud prevention workflows requiring customer interaction.

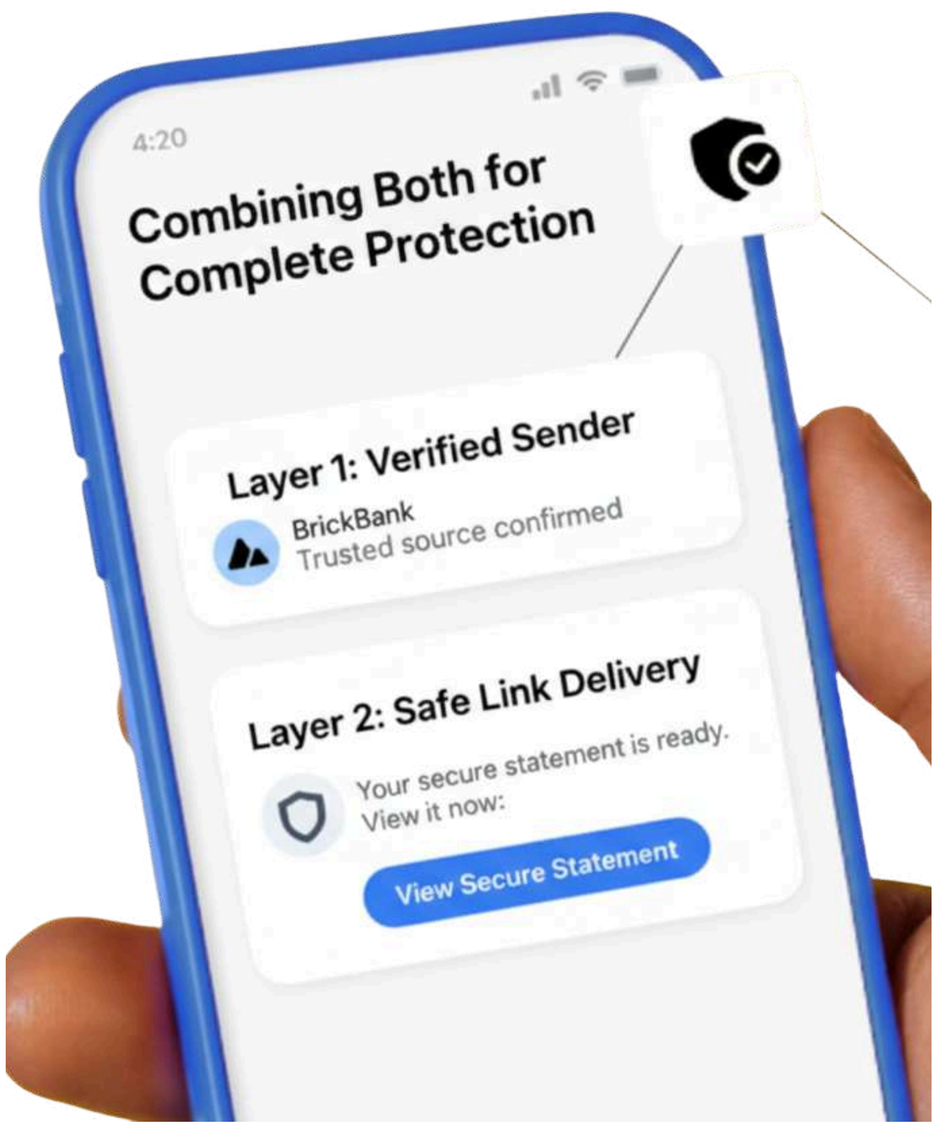
With an 8,000+ character limit, it includes rich cards with images and video, carousels with up to 10 cards, up to 4 action buttons per card, webview integration, drag-and-drop campaign builder, and advanced analytics dashboard. Implementation takes 2-5 days.

RCS Studio excels at fraud transaction review where suspicious transactions display as rich cards with merchant logos, transaction details, and action buttons for "Approve" or "Report Fraud."

It guides account compromise recovery with step-by-step rich cards showing what to do, which services to update, and how to secure accounts.

Security education becomes interactive with tutorials about recognizing scams, using authentication tools, and protecting accounts through images, examples, and quiz-like interactions.

Document verification requests identity documents for account recovery using rich cards with photo upload buttons and clear instructions.



Combining Both for Complete Protection

The most effective fraud prevention strategies use both RCS Basic and RCS Studio strategically.

RCS Basic handles high-frequency, time-sensitive alerts like transaction notifications, login alerts, password change confirmations, and OTP codes.

RCS Studio manages complex interactions including fraud investigation, account recovery, security education, and document collection.

When a customer's debit card is used for a suspicious $800 purchase, RCS Basic sends an immediate alert: ***"Card 3421 charged $800 at Electronics Store. Reply FRAUD if unauthorized."***

The customer replies ***"FRAUD"*** within 30 seconds. RCS Studio then takes over with a rich card showing transaction details, merchant information, and action buttons for ***"Block card," "Report stolen,"*** or ***"Need help."***

The customer taps ***"Block card."*** RCS Basic confirms the action: ***"Card ending 3421 is now blocked. Replacement card ships in 2-3 business days."***

Finally, RCS Studio guides recovery with a series of rich cards explaining what happens next, which automatic payments to update, and how to monitor the account for additional unauthorized charges.

Measurable Fraud Reduction **Results**

The 89% Phishing Vulnerability Reduction

Financial institutions implementing verified RCS messaging see dramatic reductions in successful phishing attempts.

The 89% figure comes from measured data across multiple US banking deployments comparing customer bases using RCS versus those still relying solely on SMS over a 12-month measurement period.

The dramatic improvement stems from clear visual authentication where customers learn to recognize verified branding and reject unverified messages, reduced confusion when all legitimate bank messages show verified branding, safe link trust where customers feel confident clicking links in verified RCS messages, and heightened scam awareness as regular exposure to verified messaging raises general security consciousness.

Call Center Volume Reduction

Fraud-related customer service calls drop significantly when RCS verified messaging is implemented. Verification calls asking "I got a text from you about suspicious activity. Is it real?" disappear when customers can visually verify message authenticity.

Customers stop ignoring legitimate fraud alerts because they thought they were scams. Fewer phishing victims mean fewer fraud resolution calls. Questions about "How can I tell if a message from my bank is real?" become unnecessary because the visual verification is self-evident.

Financial institutions implementing RCS see 40-55% reductions in fraud-related call center volume within six months, translating to substantial cost savings beyond direct fraud losses prevented.

Faster Fraud Detection and Response

When customers trust security alerts, they respond faster. Traditional SMS fraud alerts have average response times of 4-8 hours because customers are uncertain about authenticity.

RCS verified alerts get responses within minutes. When a fraudster steals card details and attempts a $1,200 purchase, the traditional SMS 6-hour response time means the charge likely processes before the customer responds.

With RCS verified messaging, the 3-minute average response time means the charge gets blocked in real time.

Faster response doesn't just prevent individual fraudulent transactions but shortens the window for criminals to exploit compromised credentials, reducing total losses per incident.

Reduced False Positive Friction

Fraud detection systems generate false positives where legitimate transactions get flagged as suspicious and customers must confirm they authorized them.

When customers don't trust fraud alerts, they ignore them, resulting in good transactions getting declined and bad transactions processing. RCS verified messaging reduces false positive friction because customers respond quickly to all alerts, sorting legitimate from fraudulent efficiently.

The bank's fraud system gets faster, more accurate feedback, which improves machine learning models and reduces future false positive rates, creating a virtuous cycle of better fraud detection.

Implementation in the **US Market**

Carrier Coverage and Compatibility

RCS availability in the US market has expanded significantly, with major carriers including T-Mobile, AT&T, and Verizon supporting RCS messaging and covering approximately 90% of US mobile subscribers.

Google Messages, the default messaging app on most Android devices in the US, fully supports RCS, meaning customers with Android phones receive verified RCS messages without downloading additional apps or changing settings.

For customers on devices or carriers that don't support RCS, automatic SMS fallback ensures universal message delivery.

RCS Basic messages fall back to standard SMS text, while RCS Studio rich messages fall back to SMS with a link to view rich content through a mobile web page.

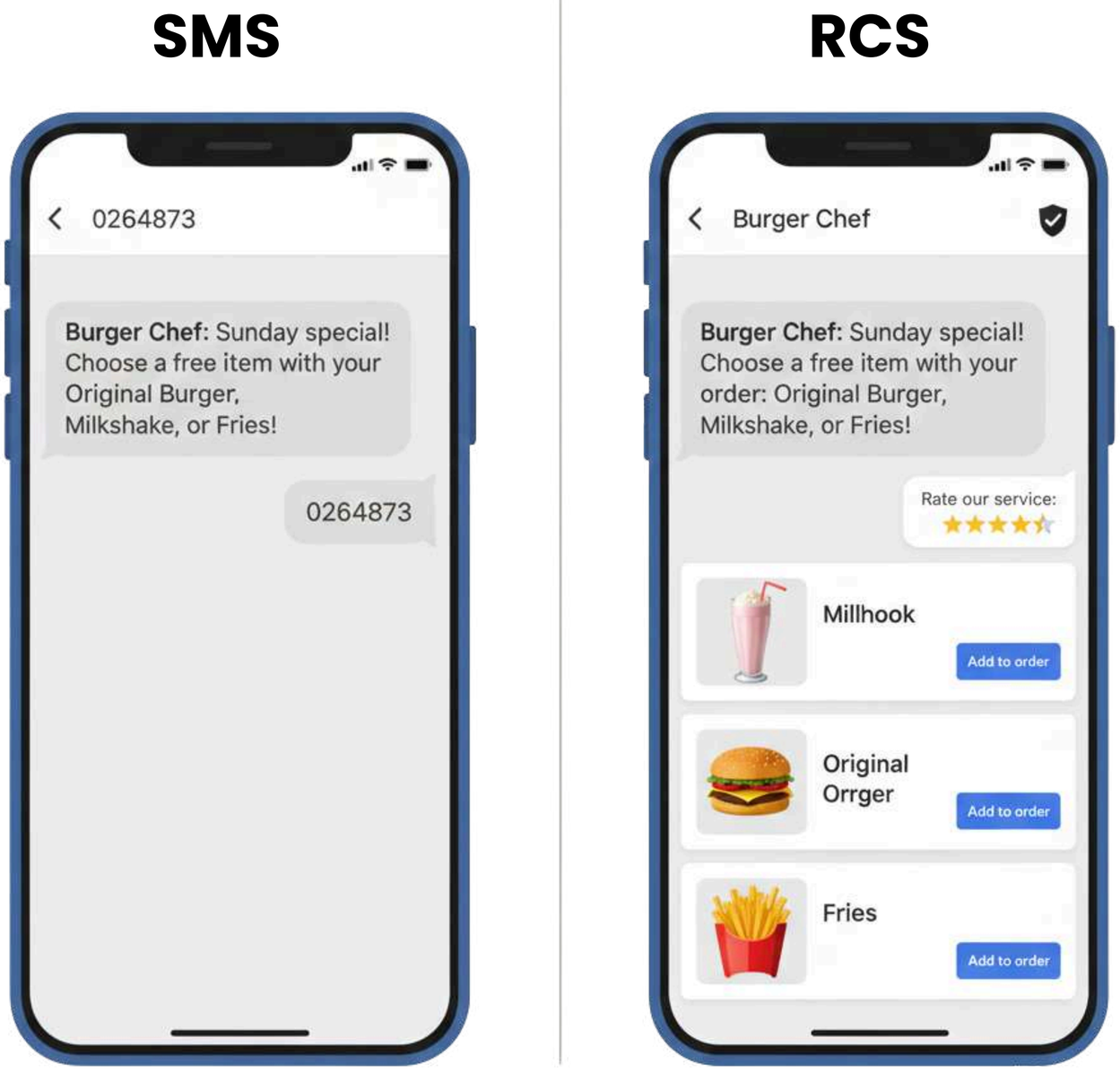
Regulatory Compliance

US financial institutions implementing RCS for fraud prevention must navigate specific regulatory requirements.

The Telephone Consumer Protection Act requires prior express written consent for promotional messages, but transactional messages for fraud alerts, account security notifications, and authentication codes don't require prior consent as they're essential to service delivery.

The Gramm-Leach-Bliley Act mandates protection of customer financial information, requiring RCS implementations to encrypt messages in transit, secure customer data at rest, and implement access controls meeting GLBA standards.

The Federal Financial Institutions Examination Council provides guidance on authentication in internet banking, and RCS verified messaging aligns with FFIEC multi-factor authentication recommendations by combining something the customer has (their verified phone number) with carrier-level sender verification.



For consumer accounts, Regulation E requires financial institutions to investigate and resolve unauthorized transaction claims, and RCS verified messaging creates clear audit trails of fraud alerts sent, customer responses, and actions taken, strengthening compliance documentation.

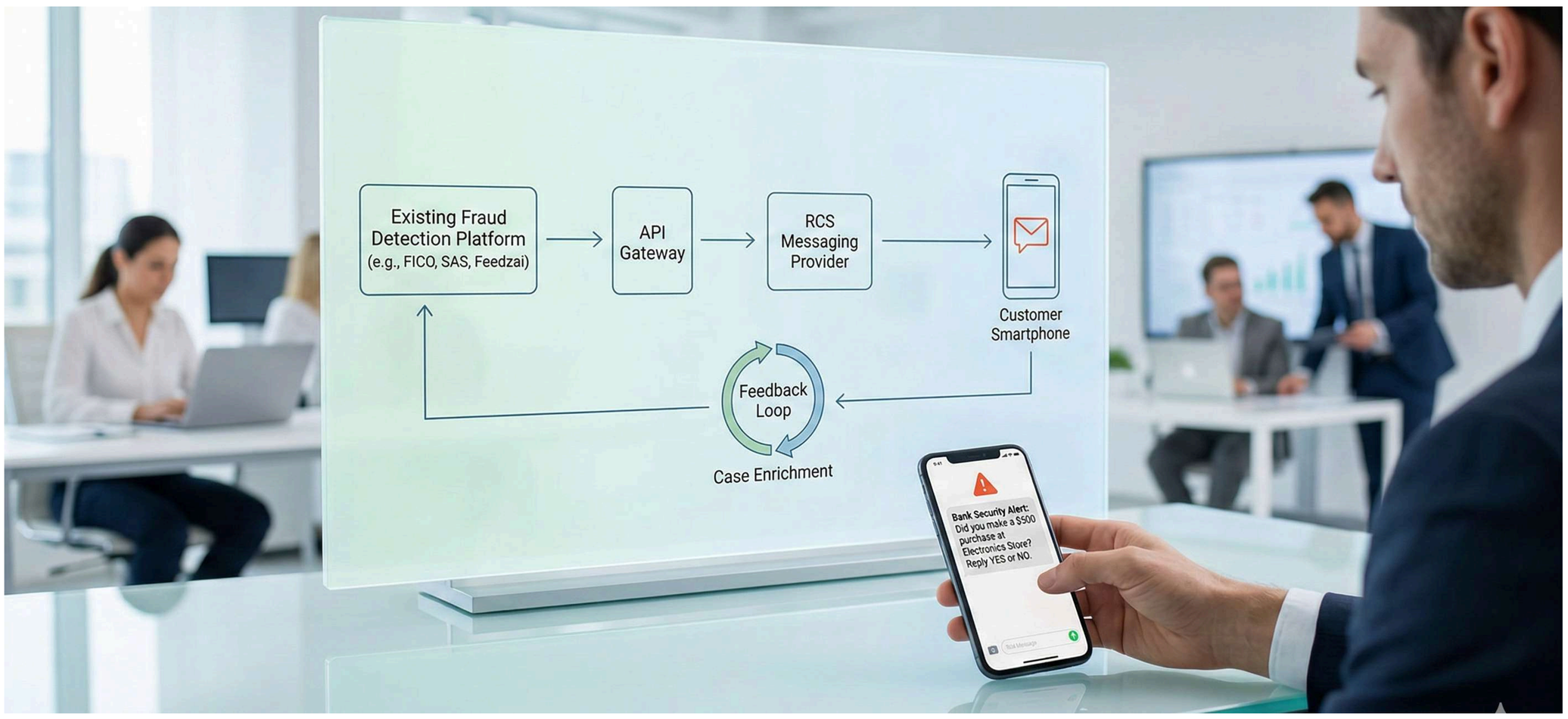
Integration With Existing Fraud Systems

RCS messaging doesn't replace existing fraud detection infrastructure but integrates with it, providing a more effective communication channel for alerts and customer interaction.

Most US banks use fraud detection platforms from vendors such as FICO, SAS, or Feedzai that analyze transaction patterns, flag suspicious activity, and trigger alerts across various channels.

RCS integration happens through APIs that connect fraud detection platforms to RCS messaging providers. When suspicious activity is detected, the fraud system triggers an RCS message instead of or in addition to SMS, email, or push notification.

The integration includes alert routing, where the fraud detection system determines which customers should receive RCS versus SMS based on device compatibility, response handling, where customer responses flow back to the fraud detection system automatically, case enrichment, where RCS read receipts and customer interaction data enhance fraud case records, and feedback loops where customer responses help train fraud detection models.



Implementation is straightforward for banks with modern fraud platforms that support API-based alert distribution, with integration timelines typically ranging from 2-4 weeks depending on existing system architecture.

Customer Education and **Adoption**

Teaching Visual Verification

The effectiveness of RCS fraud prevention depends on customers understanding and trusting verified branding.

Education happens through multiple channels including first-message introduction explaining verified messaging, in-branch materials with posters and handouts, online banking notices educating customers about verified messaging, transaction receipt education with brief reminders, and proactive scam warnings when phishing campaigns are detected.

The education doesn't need to be technical. The message is simple: "Real messages from us have this logo and badge. Messages without them are scams."

Building Trust Through **Consistency**

Customer trust in verified messaging builds through consistent, positive experiences.

Every verified RCS message reinforces the pattern customers should expect. This means all legitimate bank communications should use RCS when possible, including transaction confirmations, balance alerts, payment reminders, appointment confirmations, account notifications, security alerts, and product offers with appropriate TCPA consent.

Consistency matters because if customers receive some legitimate messages through verified RCS and others through unverified SMS, the education breaks down and they become confused about which channel is official.

Advanced Fraud Prevention **Workflows**

Real-Time Transaction Verification

RCS Studio enables sophisticated transaction verification workflows that would require phone calls or app interactions through traditional channels.

When a high-risk transaction is flagged, instead of a simple "Was this you?" SMS, customers receive a rich card showing merchant name and logo, transaction amount and date, location information if available, and action buttons for "I made this purchase," "This is fraud," or "Not sure."

If the customer taps "This is fraud," a follow-up card appears with options to block the merchant from future charges, block the card immediately, report the card as lost or stolen, or speak with a fraud specialist.

The entire investigation and resolution happen within the message thread without phone calls, app downloads, or separate authentication steps.

Account Takeover Prevention

Account takeover attempts generate distinctive patterns including sudden password changes, addition of external accounts for transfers, changes to contact information, or unusual login locations.

RCS verified messaging enables real-time intervention asking "We noticed a password change from an unrecognized device in California. Was this you?"

If the customer responds "No," immediate protective actions trigger including password reset required, active sessions terminated, account temporarily locked, and fraud team notified.

If the customer doesn't respond within 5 minutes, escalating protections activate automatically based on risk level. The key is speed because account takeover criminals work fast, moving money out of compromised accounts within minutes.

Cost-Benefit **Analysis**

Direct Fraud Loss Prevention

The primary financial benefit of RCS verified messaging is prevented fraud losses.

For a regional bank with 500,000 customers typically seeing 800-1,200 successful phishing incidents annually at an average cost of $1,200-1,800 per incident, total annual fraud losses from phishing run $960,000-2,160,000.

With 89% reduction in phishing vulnerability, prevented losses reach $854,000-1,922,000 annually.

Call Center Cost Reduction

Fraud-related customer service calls are expensive, with a regional bank with 500,000 customers fielding 50,000-75,000 fraud-related calls annually at an average cost of $5-7 per call, totaling $250,000-525,000.

With 40-55% reduction in fraud-related call volume through RCS implementation, savings reach $100,000-288,000 annually.

Customer Retention Value

Customers who fall victim to fraud while banking with an institution often leave, with customer attrition rates after fraud victimization running 15-25%.

If RCS prevents 850 phishing incidents annually, that's potentially 128-213 fewer customers lost to fraud-driven attrition.

At an average customer lifetime value of $2,500-4,000, retained customer value reaches $320,000-852,000 annually.

Implementation and Operational Costs

RCS messaging costs are modest compared to benefits. For a bank sending 5 million security messages annually, mostly through RCS Basic with 10% through RCS Studio, total messaging costs run approximately $10,000-20,000 annually.

Initial setup fees for carrier verification, platform integration, and workflow development typically range from $15,000-40,000. Platform management, campaign creation, and analytics typically require 10-20 hours monthly of staff time, representing $20,000-40,000 annually in labor costs.

Total annual cost runs approximately $45,000-100,000 for a regional bank deployment. Benefits of $1,274,000-3,062,000 minus costs of $45,000-100,000 yield net benefit of $1,229,000-2,962,000 annually. The payback period is measured in weeks, not years.

Conclusion

SMS phishing costs US financial institutions and their customers over $330 million annually in direct losses, with indirect costs running several times higher. Traditional SMS provides no defense against this threat because it offers no sender authentication.

RCS verified messaging solves the fundamental problem where customers can't tell legitimate messages from scams. With verified branding including logos and trust badges at the carrier level, customers learn to recognize authentic communication and reject spoofed messages.

The measured results are compelling: 89% reduction in phishing vulnerability, 40-55% reduction in fraud-related call center volume, faster fraud detection and response, and substantial cost savings that far exceed implementation costs.

For US financial institutions, the question isn't whether to implement RCS verified messaging but how quickly you can deploy it to protect customers and reduce fraud losses.

our customers are being targeted by sophisticated phishing operations right now. Every day without verified messaging is another day they're vulnerable to scams impersonating your institution.

The technology exists, the business case is clear, and implementation timelines are measured in days or weeks. The barriers to deployment are minimal. The benefits are substantial and immediate.

RCS Studio from Signalmash makes verified messaging implementation straightforward for US financial institutions. Our platform provides both RCS Basic for efficient, verified transactional messaging and RCS Studio for rich, interactive fraud prevention workflows.

With implementation timelines of 1-2 days for RCS Basic and 2-5 days for RCS Studio, you can start protecting customers and preventing fraud losses within a week.

We handle the complexity of carrier verification, regulatory compliance, and platform integration. You focus on protecting customers and reducing fraud losses.

The future of banking security is verified communication that customers can trust. Give your customers the protection they deserve. Stop letting scammers impersonate your institution. Implement RCS verified messaging and reduce phishing vulnerability by 89%.

Contact Signalmash RCS Studio today to discuss how verified messaging can protect your customers and reduce fraud losses at your institution.

Contact Information

Experience_RCS@signalmash.com

Toll-Free: +1 866 217 9750 Local and International: +1 971 369 7740

Primary Address: 3000 NE Stucki Ave, Ste 230 Hillsboro, OR 97124

Document Version: 1.0
Publication Date: March 2026