



The currency of trust:

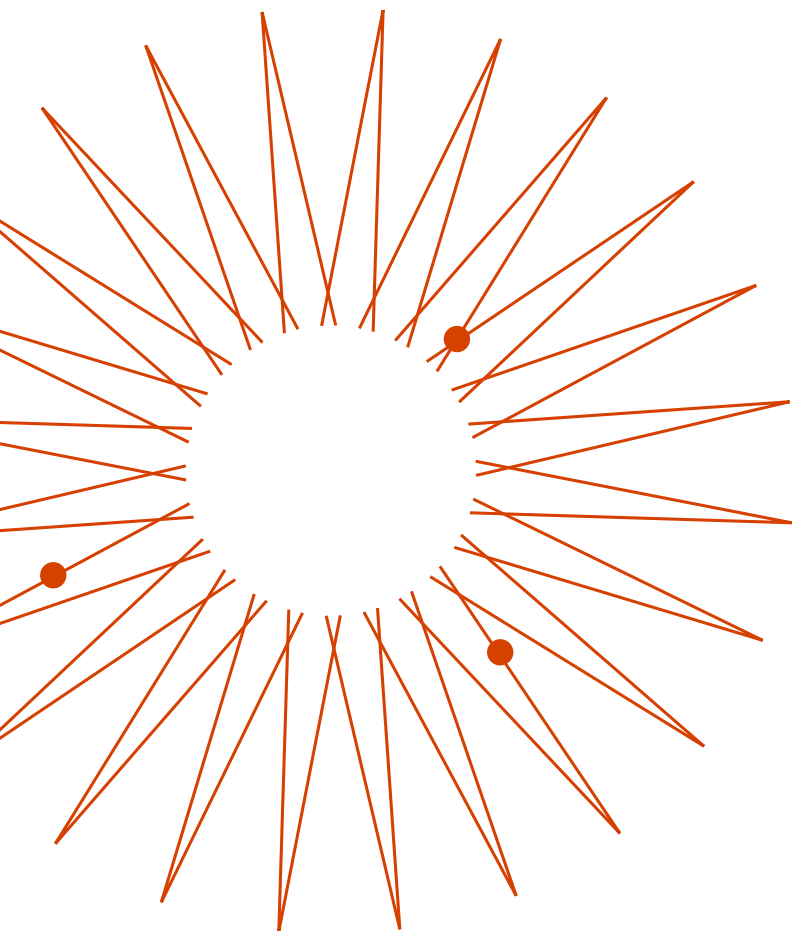
Securing the audit
confirmation process





Contents

Executive summary	3
The evolution of financial cybercrime	4
Historical failures of social engineering and verification	5
The hidden hazards of second-rate confirmation channels	7
The auditor's imperative: Defensibility	9
Thomson Reuters Confirmation: The industry-leading solution	10



Executive summary

Our modern banking environment is dominated by multi-factor authentication, biometric access controls, and predictive fraud detection. Yet, a quiet and highly vulnerable workflow continues to expose financial institutions to severe risk: the audit confirmation process.

Audit confirmations are the formal, independent verification of corporate balances, liabilities, and complex credit facilities. They're essential to the integrity of global financial markets. However, the methods used to transmit this highly sensitive information are frequently outdated.

As cybercriminals leverage sophisticated social engineering tactics, generative AI, and advanced Business Email Compromise (BEC) techniques, relying on unencrypted email or secondary, low-security confirmation partners creates an unacceptable risk.

This e-book explores the urgent security demands of the modern audit confirmation process, examines the systemic failures of the past, analyzes the dangers of subpar verification networks, and provides a clear framework for secure, automated, and audit-defensible data stewardship.



The evolution of financial cybercrime

For corporate banking clients, security is the ultimate measure of institutional value. Financial institutions invest billions of dollars annually to protect their perimeters, yet corporate data remains exceptionally vulnerable at the boundary lines where financial institutions share information with external third parties, such as auditors.

The Zero Trust mandate in third-party exchanges

Modern cybersecurity architecture has transitioned from a perimeter-based "castle-and-moat" model to a strict **Zero Trust framework**: never trust, always verify. Under a Zero Trust model, no user, device, or communication channel is trusted by default, regardless of whether it originates inside or outside the bank's network perimeter.

This framework is critical during the audit confirmation lifecycle. Traditionally, if an incoming email appeared to come from a known accounting firm, bank employees completed the request in good faith. Today, a Zero Trust approach requires that every request, auditor identity, authorizing signature, and destination endpoint be dynamically and independently verified before any customer financial data is disclosed.

The rise of generative AI and synthetic phishing

The threat landscape has evolved rapidly with

the advent of generative AI. Attackers no longer rely on easily detectable, grammatically flawed phishing emails. Instead, they leverage large language models (LLMs) to write flawless, **highly persuasive communications** that mimic the precise professional tone and terminology of legitimate audit partners.

Furthermore, bad actors use generative AI to **clone the voices** of senior corporate treasury officers or generate synthetic authorization documents. When these tactics are deployed against banks relying on unencrypted email or basic web portals, staff can easily be manipulated into releasing non-public personal information (NPI).

Global regulatory fragmentation and data sovereignty

Banks must also navigate a complex, fragmented web of international data sovereignty laws. Frameworks such as the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) heavily penalize unauthorized data disclosures, regardless of whether they occurred via a malicious external hack or an accidental leak to an unvalidated third party.

Because corporate audits frequently cross international borders, a bank must ensure its confirmation pipeline complies with local data residency and transmission laws. Failing to do so can result in massive regulatory fines and direct legal liability.

Historical failures of social engineering and verification

The risks associated with unsecure audit confirmations are not theoretical. The history of corporate finance contains major scandals where weak confirmation practices, social engineering, and intercepted communications enabled multi-billion-dollar frauds.

The Wirecard collapse: A legacy channel failure

In 2020, German fintech giant Wirecard AG collapsed after auditors discovered that €1.9 billion in cash, supposedly held in escrow accounts at Asian banks, did not exist. The fraud was covered up for years because the verification process relied on third-party trustees and unverified, easily manipulated paper and email chains.

This historic failure showed how relying on unsecure communication paths allows bad actors to manipulate confirmations and hide massive financial fraud. Read the details in the Reuters [coverage of the Wirecard collapse](#).

The Satyam scandal: Fabricated bank letters

In India's "Satyam scandal," the chairman of Satyam Computer Services admitted to inflating the company's cash and bank balances by over \$1 billion. The fraud was kept alive using thousands of fabricated bank confirmation letters printed on fake letterhead, which were sent to auditors without direct validation from the financial institutions.

This case highlights why direct, secure, and independent verification is necessary to prevent social engineering. Review the official SEC filings in the [SEC's Satyam litigation release](#).





The Parmalat crisis: Intercepted communications

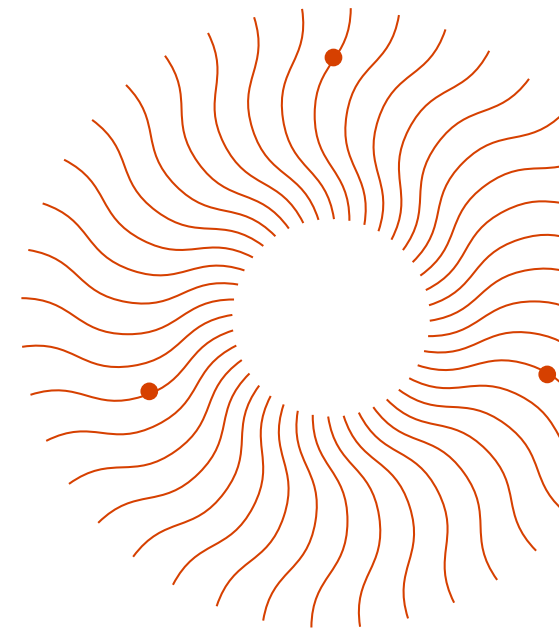
In Europe, dairy conglomerate Parmalat went bankrupt after a €3.9 billion hole was discovered in its accounts. A key element of the fraud was a fake document, ostensibly from Bank of America, confirming a cash balance that did not exist.

The fraudsters used a simple fax machine and social engineering to intercept and forge the confirmation, showing how easily legacy transmission channels can be exploited. Read the historical context in [The New York Times' Parmalat analysis](#).

The Ubiquiti Networks BEC scam

In 2015, Ubiquiti Networks was targeted by a sophisticated Business Email Compromise (BEC) attack. Using spoofed email addresses and look-alike domains, attackers impersonated executive leadership and external partners to bypass standard verification protocols, stealing \$46.7 million.

This case demonstrates how easily cybercriminals can use social engineering to exploit standard email-based confirmation systems. Review the case details in the [SEC's report on business email spoofing](#).



The hidden hazards of second-rate confirmation channels

The evolution of audit confirmation risks



As banks look to move away from legacy methods like mail and unencrypted email, many fall into the trap of using subpar confirmation providers or unverified digital databases. These low-security networks lack the rigorous verification processes and technical protocols needed to truly protect customer data.

The security gap: Lacking SOC 1, SOC 2, and historical audits

Many secondary digital lookup platforms and transaction-only databases operate without the rigorous compliance frameworks that enterprise banks require. A premium confirmation partner must possess years of consecutive SOC 1 and SOC 2 Type II compliance reports. These reports prove that the provider's systems have been subjected to continuous, rigorous testing of their control objectives, data confidentiality, and operational integrity over a long period.



When a bank partners with a provider that lacks a proven track record of SOC compliance, it exposes itself to severe vulnerabilities. These secondary platforms often pass fewer independent security audits, leaving their backend databases vulnerable to SQL injections, credential stuffing, and unauthorized access.

The operational fallback loop

Accounting firm employees are trusted with protecting their clients' banking data and will not use a confirmation platform they don't trust. That could be due to its lack of security credentials, missing compliance reports, or poor industry reputation.

This creates an operational headache: auditors will bypass the platform and revert to sending confirmation requests via standard email or physical mail. The bank's staff is then forced back into manual, high-risk workflows, defeating the bank's investment in technology and leaving the data pipeline exposed.



Result: Bank staff reverted to manual, high-risk workflows



The auditor's imperative: Defensibility

Accounting firms are bound by strict international standards. Under regulations like **PCAOB AS 2310** (The Auditor's Use of Confirmation), **PCAOB AS 2401** (Consideration of Fraud in a Financial Statement Audit), **AICPA standards**, and **ISQM 1 & 2** (International Standards on Quality Management), auditors must use confirmation pathways that guarantee:

- **Audit defensibility:** A clear, unalterable trail showing exactly when a request was authorized, who responded, and how it was transmitted.
- **Direct communication:** Absolute assurance that the client cannot intercept, alter, or influence the data in transit.
- **Robust data retention:** Safe, reliable storage of audit evidence that complies with regulatory retention periods.

If a bank's confirmation provider cannot offer this level of compliance, auditors cannot rely on the data. This creates friction, delays audit opinions, and damages relationships with mutual clients.



Critical security questions for financial institutions

To safeguard client data and protect your institution from operational bottlenecks, you should ask potential confirmation partners these six questions:

Does this confirmation partner:

1. **Match our data** retention and security policies?
2. **Offer integrations** with our internal systems to eliminate duplicate data entry?
3. **Validate each party** on the platform to prevent unauthorized data transfer?
4. **Have the trust** of professionals around the world to eliminate time-consuming mailed, emailed, and faxed requests?
5. **Offer reliable access** during audit busy season when request volumes increase?
6. **Pass hundreds** of independent security audits annually?



Thomson Reuters Confirmation: The industry-leading solution

To mitigate these risks and achieve operational efficiency, banks must partner with a proven, enterprise-grade platform. Thomson Reuters® Confirmation is the undisputed, industry-leading provider for electronic audit confirmations, trusted by financial institutions worldwide.

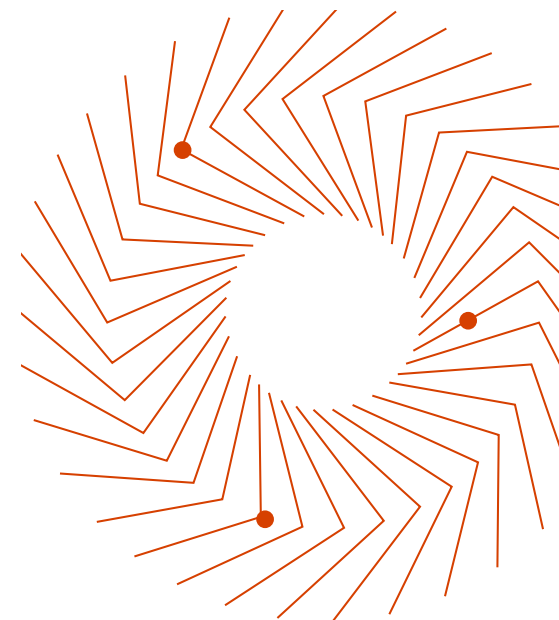
By keeping the entire verification loop within a secure, validated system, Confirmation prevents clients or bad actors from altering financial records. Confirmation has been used to uncover billions of dollars in financial statement fraud, including:

- The **\$215 million** financial fraud by [Peregrine Financial Group \(PFG\)](#)
- The **\$160 million** financial fraud by [China MediaExpress](#)
- A **7-year, multi-million-dollar** financial fraud scheme orchestrated by [James A. Shepherd](#)

Unmatched scale, experience, and global reach

As the pioneer that invented electronic confirmations over 20 years ago, Confirmation is used by more than **1.5 million professionals** and **20,000 audit firms** across **170 countries**, processing over **2.6 million confirmations annually**.

The network connects more than **4,300 banks and departments** globally. Its industry-leading status is validated by its adoption rate among premier financial institutions: **more than 580 financial institutions use the platform exclusively** as their standard operating procedure.



To support global operations, Confirmation provides:

 Dedicated account managers located across 20 offices globally.	 24/5 customer support via email, phone, and live chat across 7 global locations (US, London, Johannesburg, Mumbai, Tokyo, Sydney, and Hong Kong).	 Multi-language access in 8 languages: English, Spanish, German, French, Portuguese, Chinese Traditional, Chinese Simplified, and Japanese, with over 350 trainings conducted yearly.
 Bank-grade security and compliance: Confirmation provides a secure, end-to-end digital ecosystem that eliminates the risks of unsecure email and manual processes.	 Rigorous validation: Confirmation validates every single user on the platform through a strict verification process before they can request or send data.	 Advanced security protocols: All signatures, attachments, and completed documents are protected with AES-256 encryption, ensuring that client data is never accessed by unauthorized parties.
 Continuous compliance: Confirmation exceeds major industry security standards, passing more than 600 independent security and compliance reviews annually to match the strict policies of the world's largest banks.	 Independently audited: Confirmation's security, availability, and confidentiality controls are examined annually by an independent accounting firm under SOC 1 and SOC 2 Type II standards.	 Ongoing monitoring and response: The platform is continuously monitored for potential security events, backed by a documented incident response plan that is regularly tested.
 Tested resilience: A business continuity and disaster recovery program, reviewed and tested annually, helps ensure the platform can recover from unexpected disruptions.	 Layered physical and personnel safeguards: Data is hosted in access-controlled facilities, and personnel undergo background screening as a condition of employment.	

Confirmation: Global trust and scale

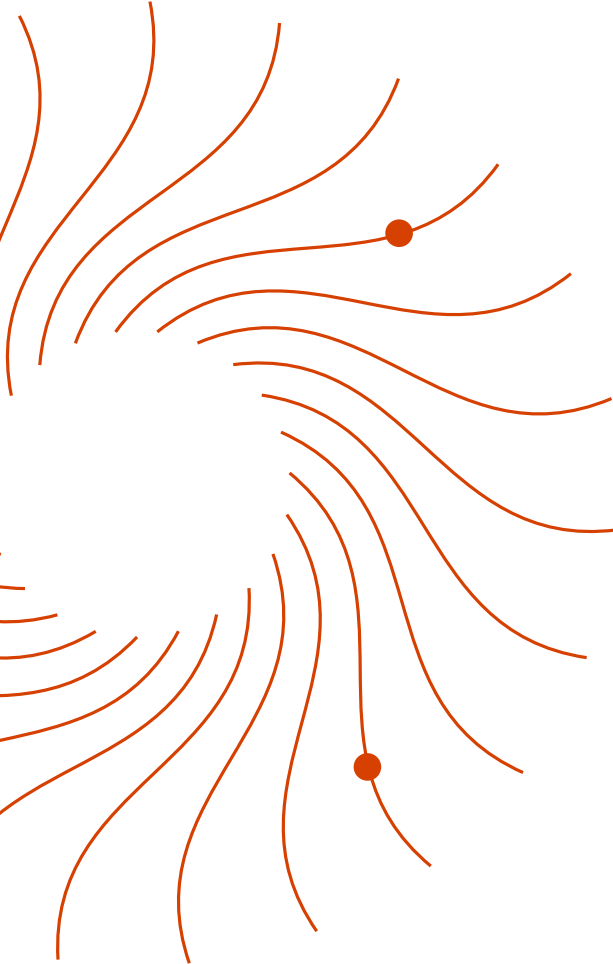
- 4,300+ financial institutions and departments
- 20,000+ registered audit firms
- 1.5 million professionals
- 87 of the top 100 U.S. banks use Confirmation
- 13 of the top 14 U.S. banks respond with Confirmation exclusively

Exceptional efficiency at no cost

While Confirmation provides enterprise-grade security, it is free for banks to use when responding to most confirmation types, including audit confirmations, bank references, reverification of mortgage, verification of deposit, and verification of mortgage. The platform charges transaction fees to the party requesting information, allowing banks to modernize their infrastructure with zero software subscription costs.

According to a **Total Economic Impact™ (TEI)** study conducted by Forrester Consulting, banks using Confirmation save an average of 50% to 60% of employee time on audit confirmations, with some reporting up to 90% time savings overall. By automating workflows, banks can delegate routine verifications to junior staff, freeing experienced employees to focus on analytical, growth-oriented, and higher-value tasks.

A **top 15 U.S. bank** struggled with the human and capital costs of processing over 30,000 confirmation requests annually. After implementing Confirmation, they realized a 90% reduction in processing costs, a 44% decrease in average response times (from 37.5 hours down to 21 hours), and 35% fewer reported confirmation errors. They successfully completed 8,000 busy-season confirmations in less than two days.



Application Programming Interfaces maximize your efficiency and security

Confirmation Application Programming Interfaces (APIs) further streamline and reduce risks associated with emailed audit and credit confirmations. Here are some of their successes:

1. **Citi:** Confirmation worked with Citi Services to modernize their confirmation response through API-driven automation. This collaboration established a new industry standard for rigor, transparency, and scalability, now live in more than 70 countries. Use of our API enables rapid and predictable onboarding into new countries. Citi Services has enhanced service delivery during audit season, improving the experience for auditors and clients alike.
2. **Interactive Brokers (IB Group):** IB Group integrated the Confirmation Auto-Process API to securely connect the Confirmation platform directly to their internal database. Today, 100% of their confirmations run automatically through the API with zero manual double work. This reduced their average response time to less than one day (often completing in mere minutes) and allowed them to handle a 52% year-over-year increase in confirmation volume with zero additional staff.

All top 5 U.S. banks use Confirmation APIs, and you could be next.

Conclusion: securing the road ahead

As fraud and data loss threats continue to scale, banks can no longer afford to treat audit confirmations as a secondary operational concern. Securing client data is a legal mandate, a financial necessity, and a competitive differentiator.

By partnering with **Thomson Reuters Confirmation**, financial institutions eliminate the risks associated with manual workflows, legacy systems, and unencrypted emails. Confirmation provides the global scale, rigorous compliance frameworks, and automated efficiency required to protect sensitive client data, detect fraud, and deliver an exceptional customer experience.

Level up your bank's security and efficiency standards today.

Visit confirmation.com to register and join the world's largest and most secure financial confirmation network.