# The evolving landscape of fraud and security threats in finance



The landscape of fraud and security threats has transformed dramatically with the advancement of technology, particularly in the realm of artificial intelligence (AI). As more individuals and businesses integrate mobile devices into their daily operations, the risk of falling victim to scams, including imposter schemes and data breaches, has escalated significantly. The Payments Journal reports on the implications of these emerging trends and technologies in this evolving environment, especially for financial institutions.

One alarming development is the rise of so-called "grandparent scams," where fraudsters impersonate a family member in distress, using AI to mimic their voice. This technique allows scammers to craft seemingly believable narratives that compel victims to send money under false pretenses. In fact, data from the Federal Trade Commission (FTC) indicates that imposter scams constituted the most prevalent form of fraud reported in 2023, with victims collectively losing over $10 million. Such scams represent a significant threat to the financial security of consumers.

The issue of call spoofing is equally concerning. Criminals engage in this deceptive practice by falsifying caller ID information to make calls appear legitimate. A common scenario involves a scammer posing as a bank employee to extract sensitive banking information from unsuspecting customers. This type of social engineering exploits the trust that individuals typically place in phone communication and has become increasingly prevalent as technology has evolved.

In parallel to these tactics, the financial sector has faced a staggering rise in data breaches. The Identity Theft Resource Center has reported that over 1,500 breaches impacted more than one billion people in the first half of 2024, marking a 14% increase from the previous year. In particular, the financial services sector saw a 67% surge in data breaches, making it the most susceptible industry. This surge correlates strongly with heightened risks for consumer fraud, as data acquired from breaches is often used to enhance the credibility of fraudulent communications.

These challenges predominantly affect smaller financial institutions like credit unions and community banks, which, according to recent findings, reported that 79% experienced direct fraud losses exceeding $500,000 in 2023. These smaller entities are often ill-equipped with the sophisticated fraud prevention resources that larger banks possess, which compounds their vulnerability given the higher personal interaction rates with customers.

On the forefront of addressing these rising threats is the implementation of technology designed to combat call spoofing. Current methods such as STIR/SHAKEN protocols are intended to authenticate callers, thereby helping consumers discern between legitimate and false calls. However, these systems face challenges due to inconsistencies in how they are implemented across various telecom networks. As a result, many legitimate calls are mistakenly identified as spam, leading to reluctance among consumers to answer their phones.

To counter these shortcomings, financial institutions can leverage additional technologies that enable them to digitally sign their outgoing calls. This development ensures that mobile operators can identify and block fraudulent calls with higher accuracy, ultimately enhancing consumer confidence in answering calls from their financial service providers.

The Payments Journal emphasises that as financial institutions take proactive measures to authenticate their calls, they not only protect their customers but also safeguard their businesses. The overarching trends reveal a pressing need for continued innovation and adaptation in security measures to counteract the evolving tactics employed by fraudsters in the digital age.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.youtube.com/watch?v=O3pD4TSJNSg> - Corroborates the rise of 'grandparent scams' where fraudsters use AI to mimic the voices of family members to trick victims into sending money.
2. <https://www.cbsnews.com/news/elder-scams-family-safe-word/> - Supports the information on AI-powered voice-cloning scams targeting older people and the financial losses associated with these scams.
3. <https://www.cbsnews.com/news/elder-scams-family-safe-word/> - Provides data from the FBI indicating that senior citizens were conned out of roughly $3.4 billion in financial crimes in 2023, highlighting the prevalence of imposter scams.
4. <https://www.netguru.com/blog/risk-reducing-ai-use-cases-financial-institutions> - Discusses the use of AI in financial institutions to detect and prevent fraud, including data breaches and other security threats.
5. <https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html> - Explains how AI-driven fraud detection and prevention models work in the banking sector, highlighting the use of historical data and real-time monitoring.
6. <https://www.netguru.com/blog/risk-reducing-ai-use-cases-financial-institutions> - Provides examples of financial institutions like HSBC, Citi Group, Deutsche Bank, JPMorgan Chase, and Mastercard using AI for fraud detection and prevention.
7. <https://www.cbsnews.com/news/elder-scams-family-safe-word/> - Details the issue of call spoofing and how it exploits the trust in phone communication, making it harder for consumers to distinguish legitimate calls from fraudulent ones.
8. <https://www.noahwire.com> - While not directly linked here, this source is mentioned in the context of the Payments Journal reporting on the implications of emerging trends and technologies in the evolving environment of financial institutions.
9. <https://www.infosysbpm.com/blogs/bpm-analytics/fraud-detection-with-ai-in-banking-sector.html> - Highlights the challenges faced by smaller financial institutions in combating fraud due to limited resources and higher personal interaction rates with customers.
10. <https://www.netguru.com/blog/risk-reducing-ai-use-cases-financial-institutions> - Discusses the importance of implementing technologies like STIR/SHAKEN protocols to authenticate callers and combat call spoofing.
11. <https://www.cbsnews.com/news/elder-scams-family-safe-word/> - Mentions the need for continued innovation and adaptation in security measures to counteract the evolving tactics employed by fraudsters in the digital age.
12. <https://www.paymentsjournal.com/fraudsters-on-the-line-the-rise-of-call-spoofing-in-the-financial-industry/> - Please view link - unable to able to access data