



AN FTI TECHNOLOGY REPORT - PUBLISHED JULY 2026

Understanding and Combating AI-Powered Fraud in Financial Ecosystems

More than [two-thirds](#)¹ of financial institutions experienced an increase in fraud events in the past year.² Generative artificial intelligence and large language models have changed the landscape, acting as threat multipliers by enabling faster, scalable creation of synthetic identities, account takeover scams and other methods of deception, with the most significant increases in AI-powered fraudulent activity in payment systems and lending scenarios. Against this backdrop, financial institutions are under pressure to adopt new approaches to detect AI scams and leverage sophisticated technology to reduce exposure.

While the concept of bad actors using the latest technology advances to accelerate malicious activity has been a risk for decades, generative AI is exponentially more disruptive. Especially in recent years, AI has transformed lending and payments fraud from messy to methodical. Today, fraudsters can use easily accessible AI to create highly plausible, consistent narratives with flawless supporting documentation across all touchpoints, including credit applications with employment letters, bank statements and explanations that align seamlessly enough to go undetected by the institution’s traditional monitoring processes. Moreover, these fraudulent profiles are repeatable at scale, allowing bad actors to simultaneously flood institutions with large volumes of fake applications or requests.

In the payments space, scammers use AI to accelerate creation of fraudulent accounts or names that imitate legitimate individuals or organisations, making it easier to trick consumers into sending a payment or providing access to their financial accounts. For example, in Brazil, the central bank’s PIX payment system, which processed approximately BRL 1.7 trillion per week in 2025, has been increasingly exploited by fraudsters using AI to steal funds or execute account takeovers that ultimately cost consumers and financial institutions significant time and cost.^{3,4} In addition to using AI to confuse consumers, bad actors are leveraging technology and AI to quickly spread funds across numerous accounts as a way to hinder traceability. The sheer scale of PIX — which regularly handles billions of transactions per month and upwards of 300 million transactions in a single day at peak — amplifies the challenge for detection and response, as fraudulent flows can be rapidly dispersed within seconds.

How AI is Changing Fraud Prevention

Aspect	Current State	Future State
Document Generation	AI generates fraudulent documents or profiles.	AI generates fraudulent documents indistinguishable from authentic ones.
Detection Capability	Forensic tools detect artefacts that signal AI generation.	Detection becomes probabilistic rather than definitive.
Fraud Response	Fraudsters refine AI prompts.	Verification will rely more on source data rather than document analysis.
Process Evolution	Detection tools improve and the cycle scales.	Evidentiary standards may need to shift.



Redefining Red Flags

The triggers banks have traditionally used to detect potential fraud have been weakened by sophisticated AI techniques. Plausibility, which has long been a pillar in financial institution review of mortgage and credit applications, is no longer a wholly reliable filter. Similarly, AI-generated loan documents have few or no obvious errors, inconsistencies or poor quality contents, attributes that current fraud prevention systems are designed to use as red flags.

In addition to the typical signals and controls, financial institutions must now implement processes that look for the absence of natural imperfections, human variations and contextual mismatches that would help differentiate fraudulent AI-generated materials from authentic documents. Such mismatches to watch for include:

- **Sophistication:** An application's contents and language complexity don't match the applicant's stated background, or the written materials cannot be conveyed verbally.
- **Lifestyle:** Claimed income doesn't match lifestyle indicators.
- **Behavioural:** Perfectly rehearsed and boilerplate responses to anticipated questions but scattered or inconsistent responses to unexpected questions.
- **Temporal:** Financial or career progressions lack natural, gradual transitions.
- **Geographic:** Claimed location doesn't match digital indicators in transaction history.

The Error Paradox

Traditional indicators are no longer sufficient in an age of AI-powered fraud, and financial institutions must become attuned to new ways of uncovering suspicious activity.

Human Indicators	AI Indicators
Poor quality document formatting, spelling errors, low resolution images.	Clean, consistent formatting.
Mathematical errors, illogical date and time sequences.	Logical calculations and consistent figures.
Contradictions between applications and supporting documents or other conflicting information.	All materials maintain the same source data.
Suspicious narratives or seemingly rehearsed explanations.	Detailed, well-thought-out narratives with supporting documentation.
Nervous behaviour, evasive responses or inability to deliver information.	Responses that are constrained to specific language and behaviours.

Addressing the Evidence Enigma

To the issue of repeatability and scalability in AI-driven fraud, systematic issues are only visible when analysing patterns across multiple applications, not within individual reviews, so instances of over-completeness and hyper-documentation should trigger suspicion and further review across a larger sample.

More, AI-enabled documentation and narrative engineering, including AI-generated or enhanced financial information, are often accompanied by coached responses during investigations, which can further confuse evidentiary assessment. Therefore, visual inspection of documents is no longer sufficient. Financial institutions must now also conduct rigorous verification, which should include:

- **Technical forensics** of sources to verify authenticity, looking at attributes such as fonts and digital signatures. Technology also helps to identify high-risk applications that warrant enhanced verification.
- **Metadata analysis** that extracts creation dates, modification history and software used to create materials submitted. This information can be compared against expected patterns for genuine bank documents and examined for inconsistencies (e.g., statement dated January 2024 but created in March 2024).
- **Transaction pattern analysis** to uncover statistical anomalies. Where genuine transactions have natural randomness, perfect patterns may be signals of AI-generated forgery. AI-powered analytics can also help detect systemic fraud across an entire portfolio, not just individual cases.
- **Granular cross-document verification.** Bank statements should be compared against tax returns and pay slips. Minor discrepancies may naturally exist, but perfect alignment across all documents could suggest AI generation from a single source.
- **Independent corroboration.** Rather than relying wholly on applicant-provided documents, institutions can request statements directly from the applicant's banks via secure channels. Bank application programming interfaces (APIs) can be used to verify account and transaction data.
- **Continuous improvement** processes to learn from detected cases and refine the approach and detection mechanisms over time.

Scaling Evidence Reliability

Reliability	Evidence Types
Highest	— Source verified data — Blockchain verified documents — Independent third party verification — Technical forensics
Medium	— Applicant-provided documents with technical verification — Testimony corroborated by independent evidence — Pattern evidence
Low	— Applicant provided documents without verification — Uncorroborated testimony — Plausible narratives
Unreliable	— Perfect consistency — Overcomplete documentation

In addition to the adjustment to more rigorous, technical review, legal and compliance teams within financial institutions must accept a mindset shift that documents cannot be assumed genuine (i.e., trust but verify). Rather, they should be considered potentially AI-generated unless verified at the source level (i.e., verify, then trust). This mindset shift can be supported in practice through the use of technology and analytics in application and fraud review, and new interview techniques that incorporate non-linear, unexpected questions with granular detail to reduce the efficacy of AI coaching during real-time interviews.

A financial institution recently encountered these issues when investigating suspected first-party lending fraud in a lender's mortgage book across the U.S., Europe and the Middle East. A team of experts examined thematic indicators

of elevated fraud risk to support enhanced fraud controls across the organisation. The investigation included:

- Six financial tests with tailored thresholds to identify customers exhibiting elevated fraud risk.
- Development and iterative refinement of sampling methodologies with regional stakeholders, adapting the approach where key data fields were unavailable.
- Manual assessment of the filtered customer population to confirm which relationships warranted a full forensic evaluation.
- Identification of critical developments to support enhancements across the fraud monitoring and investigation ecosystem.

When Employees Weaponise AI

Beyond the use of AI to create fraudulent loan and credit applications or execute account takeovers, AI is also exacerbating internal fraud risk. Employees have always had access, knowledge and opportunity to commit fraud, and AI multiplies this threat. Malicious insiders may use AI to assist in various forms of misconduct, such as expense manipulation, paid time off misuse, or misappropriation of intellectual property or funds.

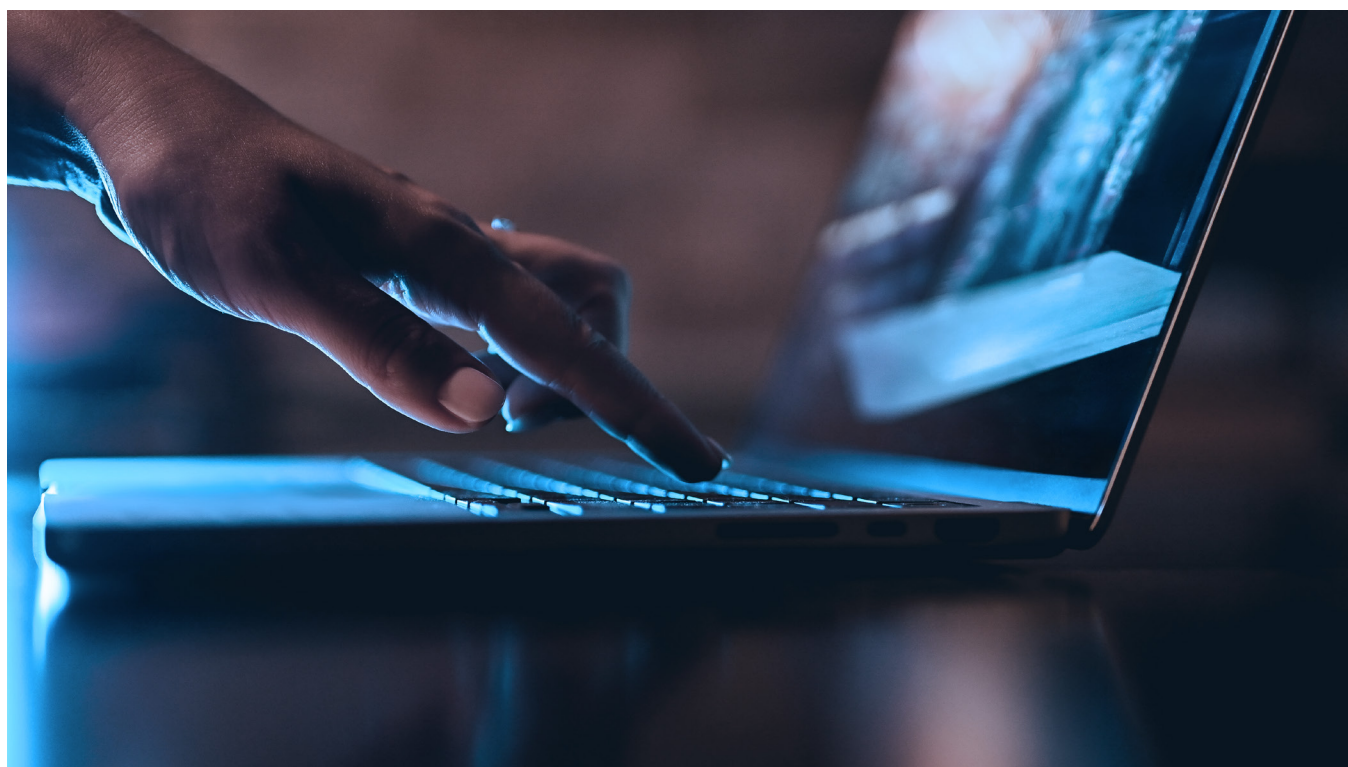
Similar to how external bad actors leverage AI to falsify documents or avoid detection by traditional filters, nefarious employees may use AI to learn how to avoid detection, receive coaching for responding to internal

auditors and create documentation that bypasses internal controls. Given how readily available and easy to use AI tools are, it is becoming much easier for individual misconduct to be scaled into systemic fraud.

As internal investigators and compliance teams adjust to the new risks of AI as a tool for employee misconduct, there are several changes to incorporate into monitoring and investigative processes.

These include:

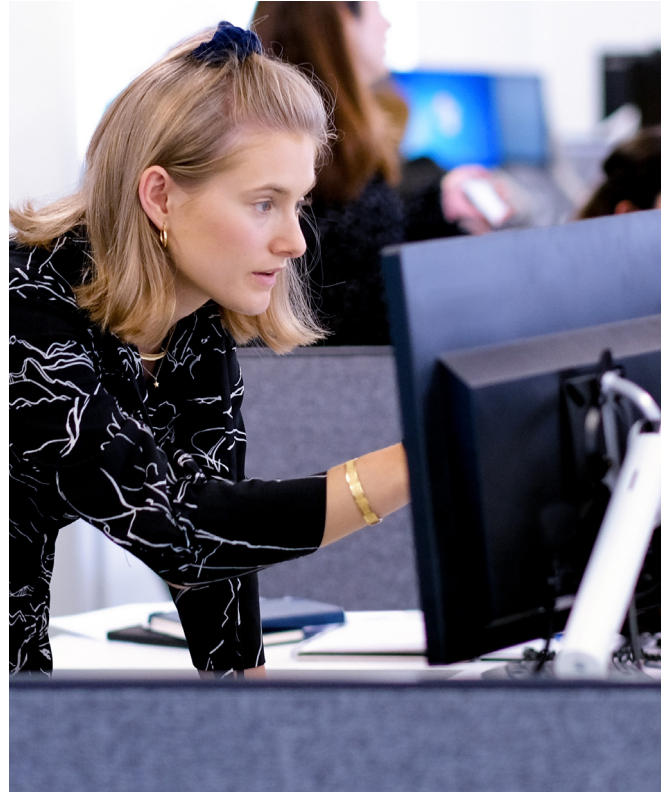
- Default scepticism, where all information or evidence is verified, not automatically trusted.
- Technical capability, including forensic skills in addition to policy and process.
- Investigative depth beyond high-risk areas, including comprehensive analysis and pattern recognition across the entire organisation.
- Evidence standards that focus on independent verification and technical forensics as the first priority, with employee testimony and documentation as secondary evidence categories.
- Sophisticated interview and inquiry techniques designed to penetrate AI coaching and scrutinise credibility.



Conclusion

Advancing technologies continually introduce new and persistent risks across financial systems. Generative AI has raised the stakes, enabling an easily accessible, fast and scalable channel for bad actors to falsify documents, create believable payments scams, steal funds undetected and subvert traditional security and compliance controls. One in five institutions lose more than \$5 million annually to successful fraud schemes and this number has grown in recent years with the rapid rise of AI.⁵

The protection and prevention layer within the financial services industry must evolve to prevent fraud losses from occurring and from growing in scope and scale. Understanding the new red flags and adjusting investigative techniques to account for them are critical first steps. The financial institutions that also shift their proactive monitoring approaches and embrace AI as a tool to support their efforts will be in the strongest position to keep pace with the changing risk landscape as AI becomes even more powerful.



Endnotes

- 1 Alloy, "2026 State of Fraud Report" (2026), <https://www.alloy.com/reports/fraud-report-2026>.
- 2 Alloy, "2026 State of Fraud Report" (2026), <https://www.alloy.com/reports/fraud-report-2026>.
- 3 Financial IT, "Pix at Five Years: How Brazil Built One of the World's Most Advanced Public Payments Infrastructures," May 2026, <https://financialit.net/news/payments/pix-five-years-how-brazil-built-one-worlds-most-advanced-public-payments>.
- 4 Williams, Lachlan, The Rio Times, "As the World Eyes Brazil's Pix, Fraud Risk Raises Red Flags," July 2025, <https://www.riotimesonline.com/as-the-world-eyes-brazils-pix-fraud-risk-raises-red-flags/>.
- 5 Alloy, "2026 State of Fraud Report" (2026), <https://www.alloy.com/reports/fraud-report-2026>.

Richard Palmer

Senior Managing Director
+44 7817 089 216
richard.palmer@fticonsulting.com

Martin Tupila

Senior Managing Director
+65 6506 9880
martin.tupila@fticonsulting.com

Veeral Gosalia

Senior Managing Director
+65 8123 5064
veeral.gosalia@fticonsulting.com

Antonio Gesteira

Senior Managing Director
+55 119 6576 9321
antonio.gesteira@fticonsulting.com

Nicholas Newbury

Senior Director
+44 20 3319 5571
nicholas.newbury@fticonsulting.com

The views expressed herein are those of the author(s) and not necessarily the views of FTI Consulting, Inc., its management, its subsidiaries, its affiliates, or its other professionals. FTI Consulting, Inc., including its subsidiaries and affiliates, is a consulting firm and is not a certified public accounting firm or a law firm.

FTI Consulting is the leading global expert firm for organisations facing crisis and transformation.

FTI Consulting is dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political and regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

© 2026 FTI Consulting, Inc. All rights reserved. fticonsulting.com