WINTER 2025

# FINANCIAL SERVICES BOARD INSIGHTS

## AI-Driven Financial Crimes Continue to Raise Red Flags

Bank security, fraud prevention, compliance, and IT professionals are pressed to manage multiple challenges when combatting financial fraud, but the malicious use of generative AI (GAI) — and the rapidly escalating losses it's causing — suggest that preventing and combatting AI-related financial fraud must be a top priority now and in the future.

Deloitte's Center for Financial Services, which tallied AI-related fraud losses at $12.3 billion in 2023, predicts AI-related fraud losses in the U.S. could reach $40 billion by 2027. Why the rocket-like rise? Credit the nature of the beast. GAI & Deepfakes.

The execution of AI and GAI scams is driven by fraudsters' endless imaginations and the continuous learning capabilities of AI and GAI. "Deepfakes" — videos, audio, images or documents that are digitally altered or generated to sound or look like someone or something else — are a type of AI self-learning that constantly monitors and adapts its ability to evaluate and bypass automated fraud detection systems. This continuous evolution enables fraudsters to continuously alter and expand the scope of their financial crimes, making it difficult for banks and their customers to anticipate the "when and how" details of each next attack.

Some types of AI financial fraud may make a financial institution more vulnerable than others. For example, business email compromise (BEC) is a common scam where a fraudster hacks executives' business email accounts, then, impersonating the hacked executives, sends seemingly legitimate instructions to transfer or wire funds into criminals' accounts.

With GAI, multiple victims can be targeted with fake executive personas at the same time, exponentially increasing the risk of fraud. In 2022, the FBI's Internet Crime Complaint Center reported 21,832 instances of BEC in that resulted in $2.7 billion in financial losses.

### Keep pace with AI developments

In its 2023 report, the Financial Stability Oversight Council (FSOC) noted the importance of monitoring AI vulnerabilities and safety and soundness risks, underscoring your Board's critical oversight of plans to address growing threats from ill-intended use of AI to commit financial fraud. Suggested priorities:

- Stay aware of emerging and trending types of fraud and train and upskill employees to identify and report suspicious activities.
- Invest in processes, procedures, and technologies to develop 360-degree customer views using actual and expected relationship behaviors to bring potential red flags to the forefront faster.
- Encourage enterprise-wide, cross-functional engagement and collaboration to improve risk assessments and support internal teams and third-party vendors directly responsible for fraud-detection and protection systems and processes.
- Provision for increases in operating budgets to meet higher costs associated with risk management activities, regulatory examinations, and compliance requirements.

While AI can provide operational efficiency and support business development strategies by deepening knowledge on consumer behaviors, it can also be easily exploited to commit financial fraud. Institutions that address AI concerns not only bolster their resilience against cyberattacks but also contribute to the strength and stability of global financial networks.

Read about AI regulatory guidance for financial institutions > here.

**For a personal consultation contact your Rehmann advisor or contact Beth A. Behrend, CBCCO, CBAP at 616.975.4100 or beth.behrend@rehmann.com; or Jessica Dore, CISA, at 989.797.8391 or jessica.dore@rehmann.com.**

## Resources for Your Board: Recommendations for Financial Institution Use of AI

For decades, financial institution leadership has anticipated, planned for, and adapted to rapidly emerging technologies. AI and generative AI (GAI) are among the latest developments. While formal guidance regarding use of these technologies struggles to keep pace with innovation, regulatory agencies have been actively engaged in the process, issuing reports, recommendations, and requests for information from financial institutions and other interested parties.

Below are a few highlights from recent regulatory agency activity that may help in your financial institution's board discussions and decisions.

### June 2023: Chatbots in consumer finance (Source: CFPB)

Over 100 million consumers are expected to interact with bank chatbots by 2026 as financial institutions increasingly adopt this cost-savings function to aid in their customer service delivery. Chatbots, which simulate human-like responses without actual human interaction, have capabilities that range from simple rules-centric responses based on ladder logic and keywords to more tailored responses that are based on real customer conversations and chat logs, and then trained to evolve through algorithms.

Read CFPB chatbot guidance > here.

### March 2024: Managing Artificial Intelligence: Specific Cybersecurity Risks in the Financial Services Sector (Source: Department of the Treasury)

This report from the Department of Treasury recommends several AI best practices that organizations in the financial services sector can use to reduce cybersecurity risks and operate in a safe, sound, and fair manner. Recommended actions include:

- Embed AI-risk management in enterprise-risk management.
- Identify AI risks specific to the institution's existing controls and its use of AI.
- Assign AI risk management responsibility to a single lead or to an existing executive position, such as chief technology officer.
- Proactively approach data acquisition, privacy, and security to understand data origination and build a comprehensive inventory and mapping framework.
- Expand third-party vendor due diligence by asking vendors in-depth questions about their AI use and integration with data retention and privacy policies.

### May 2024: 2024 National Strategy for Combatting Terrorist and Other Illicit Financing (Source: Department of the Treasury)

This national strategy outlines the U.S. government's goals, objectives, and priorities to disrupt and prevent illicit financial activities amid ever-changing global geopolitical and economic conditions. It offers an evaluation of anti-money laundering and other efforts to counter the financing of terrorism (AML/CFT) threats. It also suggests how a financial institution's deployment of machine learning and generative AI can strengthen AML/CFT compliance through the rapid analyzation of large datasets. Developed in collaboration with the FDIC, FRB, NCUA, OCC, SEC and other agencies, the report notes that further study is needed to understand the extent and application of AI to identify patterns, risks, and trends that threaten the financial system.

Read the Strategy > here.

### June 2024: Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector (Source: Department of the Treasury)

Noting that AI powers many non-bank companies' capabilities and services, this RFI invited financial institutions — which it defines as any company that facilitates or provides financial products or services — to provide their perspective on the opportunities and risks that AI developments and applications present within the sector. Although the comment period closed in August 2024, and further action is pending, more than 100 comments are available for viewing. View comments > here.

### August 2024: Response to RFI (Source: American Bankers Association)

The ABA highlighted the distinction between traditional AI (which responds to specific data inputs) and GAI (which learns from data inputs and makes decisions and predictions to generate synthetic content). It also requested that regulators apply consistent guidance and requirements to banks and non-banks offering financial services. Moreover, the ABA stressed the importance of transparent and congruent customer disclosures regarding information collection, storage, sharing, and use.

Read the ABA response > here.

**Want to offer more perspective and actionable steps to guide your board members in addressing AI? Click here.**

The regulatory landscape for financial institutions' use of AI continues to progress. Contact your Rehmann advisor for a personal consultation or contact Joe Sarnicola at joe.sarnicola@rehmann.com or 616.975.4100; or Jessica Dore, CISA, at 989.797.8391 or jessica.dore@rehmann.com.

## CRE Lending Regulators Focus on Internal Loan Reviews

While estimates can vary based on what source you review, most banks have CRE loans in their portfolio — the largest loan type for nearly half of all banks. The upward trajectory of CRE loan delinquencies that began in Q4 2022 continued with elevated lending exposure throughout 2023.

Trends in 2024 continued to point toward increases in delinquencies in CRE due to decreased loan growth and continuing declines in occupancy. These trends indicate pressure on management of CRE lending and have resulted in heightened regulatory attention with an increased focus on internal loan reviews.

### Your Recommended Response to CRE Lending Pressure in 2025

**The FDIC, OCC, the Fed, and NCUA agree:** An effective credit risk review function is critical to safe and sound operation. It helps financial institutions identify, evaluate, and address emerging risks associated with credit weakness. It also helps validate and adjust risk ratings before regulatory inspection.

### Be On the Lookout: Red Flags & Factors in to Consider in CRE Loan Reviews

Some common characteristics of inadequate loan review and factors that contribute to CRE lending delinquencies and losses may include:

- Failure to review the entire borrower relationship, incomplete loan file data, outdated cash flow information, and lack of proof of liquidity
- Lack of market information, out-of-market lending, and purchase of loan participations
- Highly leveraged transactions and long gestation periods that allow market dynamics to change before a project's completion
- Relatively low borrowing costs and the easy availability of credit
- Nonrecourse lending and legal structures that shield project sponsors from risk

### New Regulations in Appraisal Industry May Improve Loan Quality

Another historical contributor to CRE lending delinquencies is the previously unregulated appraisal industry that often relied on inflated assumptions from inexperienced appraisers. Now, regulated appraisals and the requirement that banks establish an independent real estate evaluation are improving lending quality. For example, new loan-to-value (LTV) limits make institutions less vulnerable to market downturns because they require borrowers to have more tangible equity in the collateral real estate to cushion against declining values.

### Updated Guidance

Updated guidance addresses concerns with and management of portfolio concentrations. It also recognizes that diversification can be achieved within CRE portfolios and differentiates risk by loan type. It targets CRE loans that use real estate-generated cash flow as the primary source of loan repayment, such as development and construction loans for which repayment depends on the sale of the property and property loans for which repayment depends on rental income.

### You May Need Heightened Risk Management Practices If ...

The guidance identifies financial institutions that may need heightened risk management practices commensurate with portfolio complexity as those with rapid CRE loan growth, concentrated exposure to certain types of CRE, or those approaching or exceeding at least one of the following supervisory criteria:

- Total loans reported on the Report of Condition for construction, land development, and other land represent 100% or more of the institution's total capital.
- Total CRE loans represent 300% or more of the institution's total capital and a 50% or higher increase in the outstanding balance of the institution's CRE loan portfolio during the prior 36 months.

These banks will receive closer regulatory attention. Underscoring the importance of internal loan review, examiners will carefully consider the financial institution's own analysis of its CRE portfolio, including:

- Portfolio diversification across property types and geographic location
- Underwriting standards
- Level of pre-sold units or other types of take-out commitments on construction loans
- Portfolio liquidity to sell or securitize exposures on the secondary market

### Loan Review Best Practices

For a solid loan review analysis, look to outsourced third-party experts, an experienced in-house team that's independent from lending and approval functions, or a combination of the two. No matter who conducts the analysis, complete documentation that supports loan review conclusions is essential.

**People.** Qualified loan review personnel should have experience in commercial lending and credit analysis, including the ability to review and understand borrower financial statements; in-depth knowledge of internal policies and state and federal regulations; and expertise establishing and managing reserves and problem loans.

**Process.** Ensure that there is a well-established process to maintain and update loan files to provide missing and stale documents, track credit downgrades, and analyze document exception patterns to identify and remediate process gaps, correct mistakes, and enhance employee training.

**Portfolio**. Individual loan reviews build the dataset for portfolio analyzation, enabling your institution to identify risks that should be monitored on an ongoing basis —before they become problems that result in delinquencies and losses. For example, human and AI-assisted evaluation of client relationships and borrowers' business cycles, as well as financial forecasts and projected and actual changes in project completion and incoming-producing property leases can support analysis of borrowers' cash flow changes that have the potential to increase delinquencies.

**Empower your board with the right tools and expertise to navigate the complexities of CRE lending. To learn more about best practices and how we can support your institution in maintaining a safe and sound operation, contact your Rehmann advisor or Liz Ziesmer at liz.ziesmer@rehmann.com or 616.975.2855; or Chris Plaskewicz at chris.plaskewicz@rehmann.com or 616.975.2809.**

## Enhancing Security with Multi-Factor Authentication (MFA)

In today's digital age, cybersecurity is more critical than ever. With the increasing number of cyber threats, protecting sensitive information and systems has become a top priority for individuals and financial institutions alike. One of the most effective measures to enhance security is multi-factor authentication (MFA).

MFA adds an extra layer of protection to the login process, making it significantly harder for unauthorized users to gain access to accounts and systems. By requiring multiple forms of verification, such as a password and a one-time code sent to a mobile device, MFA ensures that even if one factor is compromised, the account remains secure. Security experts widely agree that MFA is a key factor in safeguarding digital assets. For financial institution board directors, understanding and implementing MFA is crucial.

### Understanding Multi-factor Authentication (MFA)

Multi-Factor Authentication (MFA) enhances security by requiring multiple methods of verifying identity. These methods are typically categorized into three main types:

**Something you know:**

- Password: A secret word or phrase used to gain access.
- Personal Identification Number (PIN): A numeric code used for authentication.
- Security Question: A question only the user should know the answer to.

**Something you have:**

- Smartphone: Often used to receive a one-time code via SMS or an authentication app.
- Security Token: A physical device that generates a unique code.
- Smart Card/ID Badge: A card with embedded credentials used for access.

**Something you are:**

- Fingerprint: Biometric verification using a fingerprint scan.
- Retinal Scan: Biometric verification using a scan of the retina.

By requiring multiple authentication factors, MFA ensures that even if one factor (such as a password) is compromised, unauthorized access is still blocked. This layered security approach is crucial as attackers develop increasingly sophisticated methods for stealing credentials. For example, even if a hacker obtains your password, they would still need access to your smartphone or biometric data to gain entry.

### Implementing Multi-Factor Authentication (MFA)

When implementing MFA, it is essential to prioritize public-facing services such as email, remote access solutions, banking accounts, and other cloud applications. These services are particularly vulnerable because they can be accessed from the internet, making them prime targets for cyberattacks like phishing and brute force attacks. Enabling MFA on these services adds an extra layer of protection, making it significantly harder for unauthorized users to gain access. Securing these high-risk entry points is a critical first step.

Here are some key steps to effectively implement MFA:

1. **Identify High-Risk Services:** Start by identifying which services and applications you use are most vulnerable to attacks. As mentioned, public-facing services should be at the top of the list.
2. **Choose Appropriate MFA Methods:** Select the MFA methods that best suit your institution's needs. This could include SMS-based codes, authentication apps, hardware tokens, or biometric verification.
3. **Integrate MFA with Existing Systems:** Ensure that the chosen MFA solution integrates seamlessly with your existing IT infrastructure. This might involve working with your IT team or a third-party provider to implement the necessary changes.
4. **Educate and Train Users:** Educate your employees or users about the importance of MFA and how to use it. Provide training sessions and resources to help them understand the new authentication process.
5. **Monitor and Adjust:** Continuously monitor the effectiveness of your MFA implementation. Be prepared to adjust based on user feedback and any emerging security threats.
6. **Enforce MFA Policies:** Implement policies that require the use of MFA for accessing critical systems and data. Ensure compliance through regular audits and by making MFA a mandatory part of your security protocols.

By following these steps, institutions can significantly enhance their security posture. Implementing MFA is not just about adding an extra step to the login process; it's about creating a robust defense against increasingly sophisticated cyber threats.

### The Role of Cyber Insurance

Cyber insurance is crucial for mitigating financial risks associated with cyber threats. Implementing Multi-Factor Authentication (MFA) can significantly impact insurance premiums and coverage. Institutions without MFA may face higher premiums or even lose coverage, as insurers view MFA as essential for reducing the risk of unauthorized access and data breaches. By adopting MFA, institutions not only enhance their security posture but also secure more favorable insurance terms, making it a critical component of any modern security strategy.

In an era where cyber threats are increasingly sophisticated, implementing Multi-Factor Authentication (MFA) is essential for protecting sensitive information and systems. MFA not only enhances security by adding multiple layers of verification but also plays a crucial role in securing favorable cyber insurance terms. By integrating MFA with modern applications and leveraging third-party providers, your institution can streamline user access and improve productivity.

At Rehmann, we understand the complexities of cybersecurity and the importance of a robust MFA strategy. Contact us today to learn how Rehmann can support your institution in implementing a strong Multi-Factor Authentication strategy and enhancing your overall cybersecurity framework. Visit our website or reach out to Jessica Dore at jessice.dore@rehmann.com or 989.797.8391 to get started.