WILSON SONSINI

"Shadow AI" Triggers First SEC Form 8-K for Unauthorized AI Use: What Financial Institutions and Public Companies Need to Know

CONTRIBUTORS

Richard C. Blake

Demian Ahn

Joseph (Tony) Misher

ALERTS

May 28, 2026

Key Takeaways

- CB Financial Services, Inc. filed the first SEC Form 8-K under Item 1.05 triggered by an unauthorized use of an artificial intelligence (AI) tool, not an external cyberattack.
- A cybersecurity incident caused by insider misuse of AI (known as Shadow AI) should be assessed for disclosure under SEC rules.
- The four-business-day disclosure clock under Item 1.05 starts at the materiality determination, not at detection of the incident.
- Shadow AI should be considered as a cybersecurity risk as part of a company's enterprise risk management framework.
- Financial institutions face layered exposure: federal banking guidance, state breach notification laws, and class action litigation.
- Suggested actions companies could take in reaction to Shadow AI developments are included below.

Background

On May 5, 2026, a Pennsylvania-based regional bank, Community Bank, the wholly owned subsidiary of CB Financial Services, Inc. (CB), detected a cybersecurity incident caused by the use of an unauthorized AI application which exposed sensitive customer information. Unlike the usual cybersecurity incident involving an attack on the company's systems by a third-party bad actor or sabotage by an internal party, the exposure of confidential information in this case arose from the improper use of AI, presumably by a bank employee who turned to the unauthorized AI for efficiencies in handling customer information. Two days later, CB determined the incident was material and filed a Form 8-K under Item 1.05.

Notably, CB determined the incident to be **material** even though:

- It did not involve a disruption to Community Bank's operations, customer access to accounts or services, payment systems, or core information technology infrastructure.
- It was not expected to have a material impact on Community Bank's consolidated financial condition or results of operations.

The incident reflects a rapidly emerging and underappreciated organizational risk colloquially known as Shadow AI, which refers to the growing practice of employees independently using large language models and other AI tools without organizational approval or security review. These tools are often deployed with good intentions but operate outside established governance, procurement, and information security controls, creating unmonitored data flows, inconsistent privacy protections, and a fundamental lack of visibility into how sensitive information is being processed, retained, or shared.

What Happened

Based on publicly available information, the facts are as follows:

- May 5, 2026: Community Bank becomes aware of the use of an unauthorized AI-based software application to process non-public customer information.
- May 7, 2026: The bank's parent company, CB, determines the incident to be material under Item 1.05 of SEC Form 8-K "due to the volume and sensitive nature of the non-public information at issue."
- May 11, 2026: The 8-K is publicly filed with the SEC. The filing confirms that Community Bank is notifying affected customers and regulators. The number of affected customers and the specific AI application involved are not publicly disclosed.
    - The compromised data includes names, social security numbers, and dates of birth among others.

What Are the Regulatory and Legal Risks of Shadow AI

SEC Cybersecurity Disclosure Obligations
CB filed under Item 1.05 of Form 8-K, which requires public companies to disclose material cybersecurity incidents within four business days of a materiality determination. Significantly, the company determined materiality based on the sensitivity and volume of the data involved and without any operational disruption or confirmed misuse of the exposed information. In addition, although CB determined that the incident was material, it stated that the incident had not had, and was not expected to have, a material impact on consolidated financial condition or results of operations.

The incident and related disclosure serve as important reminders for public companies:

- A cybersecurity incident need not involve an external attacker or system intrusion or material financial consequences to qualify as material under Item 1.05.
- Insider misuse of technology, including unauthorized use of AI tools, can independently trigger SEC disclosure obligations if the confidential information at risk is sensitive and extensive such that a company determines the incident is material.
- The four-business-day disclosure clock begins upon a materiality determination, not upon detection of the incident.

State Data Breach Notification Laws
The exposure of names, social security numbers, and dates of birth can trigger mandatory breach notification obligations under U.S. state laws, as well as several federal regulatory frameworks applicable to financial institutions. Most state breach notification statutes impose strict deadlines, typically ranging from 30 to 90 days following discovery or determination of a breach, for notifying affected individuals and, in many states, the attorney general or a designated regulatory authority.

Litigation and Class Action Exposure
Incidents involving social security numbers and dates of birth often attract plaintiff class action interest, and the Community Bank incident is no exception. Several plaintiffs' firms have already publicly announced investigations. Affected customers may assert claims under a range of theories, including negligence, breach of implied contract, invasion of privacy, and state consumer protection statutes. In jurisdictions with statutory data breach causes of action, plaintiffs may be entitled to per-person statutory damages without needing to demonstrate actual harm, significantly increasing aggregate potential exposure.

The AI dimension of the Community Bank incident introduces additional legal complexity. The novelty of Shadow AI as a vulnerability may give rise to emerging theories of liability centered on the adequacy of an organization's AI governance framework, to include, whether the institution maintained reasonable policies governing employee use of AI tools, whether those policies were enforced, and whether the absence of technical controls constituted a failure to implement reasonable security measures. In addition to the risk of claims from affected customers, these issues also raise the risk of shareholder litigation based on a board of directors' alleged failing in supervising management or ensuring that adequate controls were in place.

While the regulatory exposure is most acute for financial institutions, the compliance risks associated with Shadow AI extend to any organization operating in a regulated industry. For financial institutions specifically, unauthorized employee use of AI tools intersects with several layers of existing regulatory obligation.

Gramm-Leach-Bliley Act (GLBA) Safeguards Rule

The GLBA Safeguards Rule requires financial institutions to implement comprehensive information security programs encompassing administrative, technical, and physical safeguards designed to protect customer information. An employee's unauthorized transmission of nonpublic customer data to an external AI platform may constitute a failure of required safeguards, potentially exposing the institution to regulatory scrutiny and enforcement by the Federal Trade Commission or applicable banking regulators.

Federal Banking Agency Guidance

The Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, and the Federal Reserve have each emphasized AI risk management as a component of third-party risk oversight and operational resilience frameworks. Examiners are likely to scrutinize whether an institution maintained adequate policies and technical controls to detect and prevent employee use of unauthorized AI applications, and whether AI-related risks were appropriately identified and addressed within the institution's broader risk management program.

New York Department of Financial Services (NYDFS) Cybersecurity Regulation (23 NYCRR 500) and Analogous State Frameworks

Financial institutions subject to the NYDFS cybersecurity regulation, and organizations subject to comparable state-level cybersecurity frameworks, are required to maintain written policies governing access controls, data classification, and the handling of nonpublic information. Unauthorized employee use of AI tools may implicate access control requirements, data classification obligations, and audit trail requirements under these frameworks, depending on the nature of the data involved and the institution's covered status.

For many organizations, the most significant near-term AI risk is not the technology itself, but the absence of governance around how employees are already using it. Sensitive data is being input into unauthorized AI tools, processed outside of established security controls, and transmitted to third-party platforms under terms of service that organizations have never reviewed. This is not a theoretical risk. It is happening now, and the Community Bank incident is among the first to have public regulatory consequences.

Recommended Actions

Know Where AI Lives in Your Organization

Organizations cannot govern what they cannot see. A meaningful AI risk management program begins with a structured inventory that maps AI components across the enterprise. For each AI asset, organizations should identify the model or service in use, how it is delivered, how deeply it is integrated into business workflows, and what data it touches. Without this foundation, organizations cannot accurately assess exposure, design effective controls, or negotiate contract protections that reflect actual risk.

Treat AI Governance and Cybersecurity as One Program, Not Two

Many organizations manage AI governance and cybersecurity as separate programs with separate teams, separate frameworks, and separate review cycles. That approach can leave gaps. AI tools can expose sensitive data, introduce access control failures, and create data flows that traditional cybersecurity controls were not designed to catch. At the same time, an AI governance policy that is not connected to your security operations and incident response program cannot be enforced through technical safeguards. Assign clear ownership, establish shared accountability between your AI and cybersecurity teams, and ensure both programs are reviewing the same risks.

Governance and Policy

- Establish an enterprise-wide AI acceptable use policy identifying authorized tools, permitted data inputs, and consequences for violations.
- Classify customer and employee data and designate which classifications are prohibited from use with external or unauthorized AI tools.
- Require AI-specific training as part of your information security awareness program, including how to identify AI features embedded in standard workplace tools.

Technical Controls

- Deploy data loss prevention tools to detect and block transmission of sensitive data to unauthorized AI platforms.
- Restrict or monitor employee access to consumer AI platforms on corporate networks.

- Maintain an approved AI vendor list and require security review and contractual data protection commitments before deployment.

Incident Preparedness

- Update your incident response plan to address unauthorized AI use, including materiality assessment triggers, escalation procedures, and notification workflows.
- For public companies, establish and test a process for evaluating materiality under Item 1.05 of Form 8-K for incidents, including those that do not involve external intrusion. Tabletop exercises simulating AI-related incidents are a practical preparedness measure.

Third-Party and Vendor Risk Management

- Review AI vendor contracts to confirm data protection, confidentiality, and restrictions on use of submitted data for model training or product improvement.
- Audit whether AI tools in use are covered by existing privacy and security frameworks.
- Do not rely on vendor certifications alone. Certifications do not guarantee that AI functionality introduced through routine product updates meets your organization's data handling requirements.

The rapid proliferation of AI tools, combined with the absence of mature governance frameworks and the persistent gap between employee behavior and organizational policy, has created a risk environment that is dynamic and consequential. The exposure organizations face today does not come only from AI tools they have chosen to deploy. It comes from tools employees are already using without authorization, vendors embedding AI into existing products, and from regulatory expectations that are evolving faster than most compliance programs can accommodate. The Community Bank incident is an early and instructive example of what that exposure looks like when it surfaces.

Wilson Sonsini works with private and publicly traded clients developing, deploying, and using AI across the regulatory spectrum, and we are actively monitoring state and federal AI laws and announcements. For more information, please contact any member of Wilson Sonsini's Public Company Representation, Artificial Intelligence and Machine Learning, and Data, Privacy, and Cybersecurity practices.