

TIM SCOTT, SOUTH CAROLINA, CHAIRMAN
ELIZABETH WARREN, MASSACHUSETTS, RANKING MEMBER

MIKE CRAPO, IDAHO
MIKE ROUNDS, SOUTH DAKOTA
THOM TILLIS, NORTH CAROLINA
JOHN KENNEDY, LOUISIANA
BILL HAGERTY, TENNESSEE
CYNTHIA LUMMIS, WYOMING
KATIE BOYD BRITT, ALABAMA
PETE RICKETTS, NEBRASKA
JIM BANKS, INDIANA
KEVIN CRAMER, NORTH DAKOTA
BERNIE MORENO, OHIO
DAVID McCORMICK, PENNSYLVANIA

JACK REED, RHODE ISLAND
MARK R. WARNER, VIRGINIA
CHRIS VAN HOLLEN, MARYLAND
CATHERINE CORTEZ MASTO, NEVADA
TINA SMITH, MINNESOTA
RAPHAEL G. WARNOCK, GEORGIA
ANDY KIM, NEW JERSEY
RUBEN GALLEGO, ARIZONA
LISA BLUNT ROCHESTER, DELAWARE
ANGELA D. ALSOBROOKS, MARYLAND

CHRIS LUCAS, STAFF DIRECTOR
JON DONENBERG, DEMOCRATIC STAFF DIRECTOR

United States Senate

COMMITTEE ON BANKING, HOUSING, AND
URBAN AFFAIRS

WASHINGTON, DC 20510-6075

October 23, 2026

The Honorable Michelle Bowman
Vice Chair for Supervision
Federal Reserve Board
20th Street and Constitution Ave NW
Washington, D.C. 20551

Dear Vice Chair Bowman:

I write regarding a supervisory policy you recently implemented, entitled “Updated Statement of Supervisory Operating Principles,”¹ that restrains bank examiners’ ability to issue supervisory warnings and execute enforcement actions to address risky conduct. Your 2026 “Cybersecurity and Financial System Resilience Report,” claims that “cybersecurity remains a top priority for the Federal Reserve.”² However, this policy leaves America’s banking system vulnerable to malicious cyberattacks, escalated by advancements in AI, by limiting bank examiners’ ability to enforce strong cybersecurity standards.³ This policy is especially harmful at a time when AI-enabled cyberattacks are intensifying and placing critical financial infrastructure at risk.⁴ As advancements in frontier AI increasingly enable bad actors to conduct cyberattacks, the Fed should be strengthening bank examiners’ supervisory tools and their ability to enforce strong cybersecurity standards, not gutting them. I write to request that you immediately rescind this policy.

The memo outlining your new supervisory policy states that “supervisory staff may issue an enforcement action based on an unsafe or unsound practice by a Board-supervised banking organization if they determine in good faith that an act or failure to act by the banking organization would...create an abnormal probability of abnormal harm to the financial condition of the banking organization...”⁵ This policy means examiners can only take action if there is “an abnormal probability of abnormal harm”⁶ and cannot take action if the likelihood of the harm is

¹ Board of Governors of the Federal Reserve System, “Updated Statement of Supervisory Operating Principles,” September 24, 2026, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260924.pdf>.

² Board of Governors of The Federal Reserve System, “Cybersecurity and Financial System Resilience Report,” September 2026, p. 4, <https://www.federalreserve.gov/publications/files/cybersecurity-report-202609.pdf>.

³ *Id.*

⁴ *Id.*; IMFBlog, “Financial Stability Risks Mount as Artificial Intelligence Fuels Cyberattacks,” Tobias Adrian, Tamas Gaidosch, Rangachary Ravikumar, May 7, 2026, <https://www.imf.org/en/blogs/articles/2026/05/07/financial-stability-risks-mount-as-artificial-intelligence-fuels-cyberattacks>.

⁵ Board of Governors of the Federal Reserve System, “Updated Statement of Supervisory Operating Principles,” September 24, 2026, p. 4, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260924.pdf>.

⁶ *Id.*

merely “possible,” if the harm is only “material” but not quite “significant,” or if the severity of the harm is uncertain. When calculating the likelihood of an incident, cybersecurity risk assessments take into account a variety of probability estimates and the “possible consequences of vulnerabilities being exercised.”⁷ Given this complex calculation and evolving AI-enabled cyberthreat capabilities, a vulnerability may not be easily quantifiable as having an “abnormal probability”⁸ of creating harm, especially if vulnerabilities have been discovered but not yet exploited.⁹ In addition, it may be difficult to quantify the level of harm that is likely to be caused by a specific cyber vulnerability or a lax cyber risk management framework, and whether that harm rises to the level of “abnormal harm to the financial condition of the banking organization.”¹⁰ This supervisory policy may prevent a bank examiner from taking supervisory or enforcement action when identifying unsafe cybersecurity practices and undermines incentives for banks to maintain rigorous policies, procedures, and internal controls related to cybersecurity.

The proliferation of AI tools that expedite phishing attempts or aid in exploiting vulnerabilities is increasingly subjecting financial institutions and their third party vendors to cyberattacks.¹¹ The potential consequences of sophisticated attacks on the financial system include operational disruption and data compromise.¹² One survey found that 76% of banks saw an increase in cybersecurity attacks over the past year and that 84% are increasing investments into cybersecurity to address risks associated with AI.¹³ Additionally, frontier AI labs like OpenAI and Anthropic have recently reported instances of cyberattacks conducted by their models during testing.¹⁴ For example, in July, OpenAI revealed that hundreds of AI agents bypassed testing guardrails, and hacked a community AI platform known as “Hugging Face,” without the company’s knowledge.¹⁵ Anthropic similarly announced that their models gained unauthorized

⁷ National Institute of Standards and Technology, “Guide for Conducting Risk Assessments,” September 2012, p. 15, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

⁸ Board of Governors of the Federal Reserve System, “Updated Statement of Supervisory Operating Principles,” September 24, 2026, p. 4, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260924.pdf>.

⁹ National Institute of Standards and Technology, “Guide for Conducting Risk Assessments,” September 2012, <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>; Board of Governors of the Federal Reserve System, “Updated Statement of Supervisory Operating Principles,” September 24, 2026, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260924.pdf>.

¹⁰ Board of Governors of the Federal Reserve System, “Updated Statement of Supervisory Operating Principles,” April 21, 2026, p. 4, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260430.pdf>.

¹¹ BIS, “When machines attack: frontier AI cyber threats and policy responses in the financial sector,” Juan Carlos Crisanto, Adrien Currat, and Jeffery Yong, September 9, 2026, <https://www.bis.org/publications/fsi-paper-28-when-machines-attack-frontier-ai-cyber-threats-and-policy-responses-financial-sector>.

¹² Board of Governors of the Federal Reserve System, “Implications of Cyber Risk for Financial Stability,” Danny Brando, Antonis Kotidis, Anna Kovner, Michael Lee, and Stacey L. Schreft, May 12, 2022, <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>.

¹³ Texas Bankers Association, “Survey shows more banks preparing for cyber attacks with AI rise,” June 24, 2026, <https://www.texasbankers.com/survey-shows-more-banks-preparing-for-cyber-attacks-with-ai-rise/>.

¹⁴ OpenAI, “OpenAI and Hugging Face partner to address security incident during model evaluation,” July 21, 2026, <https://openai.com/index/hugging-face-model-evaluation-security-incident/>.

¹⁵ OpenAI, “The Hugging Face incident and the road ahead,” August 26, 2026, <https://openai.com/index/hugging-face-incident-and-the-road-ahead/>; NBC News, “OpenAI agents hacked Hugging Face in 700-strong swarm, tried to cover tracks, investigations find,” August 27, 2026, <https://www.nbcnews.com/tech/tech-news/openai-report-says-network-was-hacked-rogue-ai-agents-rcna594590>.

access to the systems of three external organizations.¹⁶ Your supervisory policy fails to account for the evolving cybersecurity threat landscape.¹⁷ Instead, it stifles supervisory and enforcement authority despite increases in malicious AI-enabled attacks¹⁸ and security breaches as a result of unchecked frontier AI development, the consequences of which are massive.

Allowing cybersecurity vulnerabilities to fester, instead of remediating them early, could lead to more frequent and severe cyberattacks, threaten the sensitive financial data of businesses and households, and undermine the stability of the financial system. Given the elevated threats AI-enabled cyberattacks raise for the financial system, I urge you to immediately rescind this supervisory policy and instead strengthen bank examiners' ability to enforce strong cybersecurity standards. If you refuse to do so, you will share responsibility for the potential harm wrought by future cyberattacks on the banking system.

Sincerely,



Elizabeth Warren
Ranking Member
Committee on Banking,
Housing, and Urban Affairs

¹⁶ Anthropic, “Investigating three real-world incidents in our cybersecurity evaluations,” July 30, 2026, <https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals>.

¹⁷ MIT Management Sloan School, “These are the most urgent AI risks, according to 272 experts,” Kristin Burnham, July 20, 2026, <https://mitsloan.mit.edu/ideas-made-to-matter/these-are-most-urgent-ai-risks-according-to-272-experts>.

¹⁸ IBM, “IBM Study: One in Four Malicious Breaches are AI-Enabled, Costing Companies \$6 Million on Average,” July 29, 2026, <https://newsroom.ibm.com/2026-07-29-ibm-study-one-in-four-malicious-breaches-are-ai-enabled-costing-companies-6-million-on-average>.