United States Senate
COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS
WASHINGTON, DC 20510–6075

June 3, 2026

The Honorable Scott Bessent
Secretary
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Dear Secretary Bessent:

I write to request information regarding the Department of the Treasury's (Treasury) efforts to strengthen the cybersecurity resilience of the financial sector amidst the growing risks of artificial intelligence (AI)-enabled cyberattacks. Recent development of AI models, such as Anthropic's "Claude Mythos," could supercharge the ability of malicious actors to identify and exploit security vulnerabilities in software.[1] If materialized, these cybersecurity deficiencies will leave sensitive financial data vulnerable to breaches and place the broader financial system at risk of destabilizing cyber attacks. It is deeply troubling that Treasury's Wall Street deregulation agenda is leaving the financial system increasingly vulnerable to AI-enabled cyber threats, as the bank examiner workforce has been slashed and supervisory authorities used to police unsafe cyber practices are being curtailed.

Anthropic's recently announced model, Claude Mythos Preview (Mythos) is reportedly "capable of finding and exploiting hidden flaws in the software that runs the world's banks, power grids and governments."[2] It had previously only been shared with a small group of organizations as part of an effort to secure critical software before potential wider release, but Anthropic has recently announced plans to release "Mythos-class" models to customers in the coming weeks.[3] Mythos' capabilities reportedly exceed those of human developers, raising widespread concerns about keeping infrastructure safe from advanced AI-enabled cyber attacks.[4] Anthropic has also

[1] The New York Times, "Anthropic Claims Its New A.I. Model, Mythos, Is a Cybersecurity 'Reckoning'," Kevin Roose, April 7, 2026, https://www.nytimes.com/2026/04/07/technology/anthropic-claims-its-new-ai-model-mythos-is-a-cybersecurity-reckoning.html.
[2] The New York Times, "Anthropic's New A.I. Model Sets Off Global Alarms," Paul Mozur and Adam Satariano, April 22, 2026, https://www.nytimes.com/2026/04/22/technology/anthropics-mythos-ai.html.
[3] Anthropic, "Project Glasswing," https://www.anthropic.com/glasswing; Reuters, "Anthropic to roll out Claude Mythos in coming weeks, launches Opus 4.8," May 28, 2026, https://www.reuters.com/business/anthropic-roll-out-claude-mythos-coming-weeks-launches-opus-48-2026-05-28/; Anthropic, "Introducing Claude Opus 4.8," May 28, 2026, https://www.anthropic.com/news/claude-opus-4-8.
[4] The New York Times, "Banks Are Warned About Anthropic's New, Powerful A.I. Technology," Rob Copeland and Colby Smith, April 10, 2026 https://www.nytimes.com/2026/04/10/business/anthropic-claude-mythos-preview-banks.html.

predicted that other organizations will introduce models with similar capabilities within the next 18 months, further raising concerns around vulnerabilities in critical software.[5]

In 2025, financial services institutions "suffered the most data breaches of any industry…for the second [consecutive] year."[6] The most common attacks impacting financial institutions include ransomware incidents, supply chain and third-party attacks, and physical card threats like skimming.[7] Third party vendor reliance in particular has seen a recent uptick: these vendors were responsible for 30% of data breaches across all industries in 2025.[8] Further analysis has found that "many critical services that are provided by cloud service providers and cybersecurity firms…are shared across nearly all major financial institutions, creating concentrated systemic risk."[9] Increased reliance on third party vendors introduces additional attack vectors for bad actors, now equipped with advanced AI tools.

While AI-enabled attacks pose increased risk for detecting and exploiting vulnerabilities in financial institutions' and third party vendors' systems, strengthening cybersecurity regulations may introduce essential protections.[10] Bug bounty and vulnerability disclosure programs (VDPs), for example, though not required by law,[11] have shown to "significantly [enhance] the security posture" of organizations.[12] They enhance security by incentivizing the public to find and report vulnerabilities in software and are largely accepted as a best practice.[13] A Department of Defense (DoD) bug bounty program launched in 2016 resulted in the identification of more than 2,100 vulnerabilities in the DoD's system, with an average of 38 vulnerabilities identified per program.[14] Bug bounty and VDPs are an example of an opportunity to use the same AI technology that is deployed to conduct attacks for defense purposes instead. Security experts also

---

[5] The New York Times, "Anthropic's New A.I. Model Sets Off Global Alarms," Paul Mozur and Adam Satariano, April 22, 2026, https://www.nytimes.com/2026/04/22/technology/anthropics-mythos-ai.html.
[6] American Banker, "Banks remain most breached sector as attacks hit record," Carter Pape, January 29, 2026, https://www.americanbanker.com/news/itrc-2025-data-breach-report.
[7] American Banker, "Banks remain most breached sector as attacks hit record," Carter Pape, January 29, 2026, https://www.americanbanker.com/news/itrc-2025-data-breach-report; U.S. Department of Treasury, Financial Crimes Enforcement Network, "FinCEN Issues Financial Trend Analysis on Ransomware," press release, December 4, 2025, https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware.
[8] Entrust, "Securing Financial Institution Supply Chains: Identifying and Fixing Weak Links," Andy Cease and Jenn Markey, February 24,2026, https://www.entrust.com/blog/2026/02/securing-financial-institution-supply-chains-identifying-and-fixing-weak-link. s.
[9] Finance and Economics Discussion Series 2025-103, Board of Governors of the Federal Reserve System, "Cyber Vulnerabilities at Large US Financial
Institutions and Their Third-Party Service Providers," Jin-Wook Chang, Jacob Dice, Shengwu Du et al., November 25, 2025,
https://doi.org/10.17016/FEDS.2025.103.
[10] NPR, "How AI is getting better at finding security holes," Huo Jingnan, April 11, 2026, https://www.npr.org/2026/04/11/nx-s1-5778508/anthropic-project-glasswing-ai-cybersecurity-mythos-preview.
[11] UpGuard, "What are Vulnerability Disclosure Programs?," December 1, 2025, https://www.upguard.com/blog/vulnerability-disclosure-programs.
[12] Blockchains, "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry." Junaid Arshad, Muhammad Talha, Bilal Saleem et al., July 8, 2024, https://doi.org/10.3390/blockchains2030010.
[13] Hacker One, "VDP vs BBP," July 17, 2024, https://docs.hackerone.com/en/articles/8368965-vdp-vs-bbp.
[14] Blockchains, "A Survey of Bug Bounty Programs in Strengthening Cybersecurity and Privacy in the Blockchain Industry," Junaid Arshad, Muhammad Talha, Bilal Saleem et al., July 8, 2024, https://doi.org/10.3390/blockchains2030010.

argue that in the light of increasing AI-enabled attacks, standards for penetration testing, a simulation to "identify any weak spots in a system's defenses,"[15] are quickly becoming out of date.[16] Modernizing vulnerability detection regulations, including those around VDPs and penetration testing, is crucial to keeping financial institutions safe from evolving cyberattacks.

Instead, the current administration is working to deregulate big banks and loosen existing supervision standards. After President Trump's February 2025 executive order, "Ensuring Accountability for All Agencies," brought independent agencies under the control of the executive branch,[17] the Treasury Department coordinated a policy agenda for financial regulators. This includes deregulation of Wall Street, lower capital requirements at large banks, a weaker stress testing framework, looser supervision of big banks,[18] reductions to the number of examination staff,[19] and more. These changes further weaken cyber resilience of the financial system amidst growing risks.

Upon your direction,[20] the Office of the Comptroller of the Currency and Federal Deposit Insurance Corporation recently proposed a rule to severely narrow the definition of "unsafe or unsound" practice, which will further limit the ability of bank examiners to use critical supervisory and enforcement tools to address cyber vulnerabilities.[21] While the rule concedes that "unsafe or unsound practice could include critical infrastructure or cybersecurity deficiencies," the narrowed definition means examiners can only take action if it is "likely," rather than merely "possible" or "plausible," that a cybersecurity incident could materially harm the financial condition of an institution.[22] 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."[23] Given this complex calculation, a vulnerability may not be

---

[15] Cloudflare, "What is penetration testing? | What is pen testing?" https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/.
[16] Forbes, "Mythos Has Banks In A Panic. If Banks Are Worried, We Should All Be," Charles Radclyffe, April 17, 2026, https://www.forbes.com/sites/charlesradclyffe/2026/04/17/mythos-has-banks-in-a-panic-if-banks-are-worried-we-should-all-be/.
[17] The White House, "Ensuring Accountability for All Agencies," February 18, 2025, https://www.whitehouse.gov/presidential-actions/2025/02/ensuring-accountability-for-all-agencies/; NAFSA, "Executive Order 14215 of February 18, 2025: Ensuring Accountability for All Agencies," February 24, 2025, https://www.nafsa.org/regulatory-information/executive-order-14215-february-18-2025-ensuring-accountability-all-agencies.
[18] Americans for Financial Reform, "Trump Administration's Banking Deregulation Puts Entire Economy at Risk," Maya Jenkins, April 20, 2026, https://ourfinancialsecurity.org/news/trumps-risky-banking-dereg/.
[19] The Wall Street Journal, "Federal Reserve to Reduce Bank Supervision Staff by 30%," Dylan Tokar and Nick Timiraos, October 30, 2025, https://www.wsj.com/economy/central-banking/federal-reserve-to-reduce-bank-supervision-staff-by-30-84fcd65f.
[20] U.S. Department of Treasury, "Treasury Secretary Scott Bessent Remarks before the American Bankers Association," April 9, 2025, https://home.treasury.gov/news/press-releases/sb0078.
[21] Office of the Comptroller of the Currency, "Defining 'Unsafe or Unsound Practice' and Revising the Framework for Issuing Matters Requiring Attention and Other Supervisory Communications: Interagency Notice of Proposed Rulemaking," October 7, 2025, https://www.occ.treas.gov/news-issuances/bulletins/2025/bulletin-2025-29.html.
[22] Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, Federal Register Notice, "Unsafe or Unsound Practices, Matters Requiring Attention," October 30, 2025, https://www.federalregister.gov/documents/2025/10/30/2025-19711/unsafe-or-unsound-practices-matters-requiring-attention.
[23] National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," September 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

easily quantifiable as "likely," especially if vulnerabilities have been discovered but not yet exploited.[24] In addition, it may be difficult to quantify whether a specific cyber vulnerability, or a lax cyber risk management framework, is likely to "materially harm the financial condition" of the bank.[25] The rule also downplays the significance of supervisory review of policies, procedures, and internal controls, which can play a meaningful role in setting the parameters for a bank's cyber risk management framework. The Federal Reserve's Vice Chair for Supervision has unilaterally implemented similar changes.[26] Despite the vulnerabilities exposed by Mythos, you and the banking agencies have not reversed course on this agenda; instead, you merely convened a meeting with big bank CEOs to discuss cyber risks raised by the model and requested access to the model from Anthropic.[27]

To make matters worse, the Trump administration has repeatedly undermined cybersecurity resources across sectors. For example, the Administration has fired countless technologists from government agencies,[28] which places Americans' and financial institutions' sensitive data at risk.[29] Further, in 2025, the Trump administration dismantled the Cybersecurity and Infrastructure Security Agency (CISA), cutting the workforce by almost one-third.[30] This is particularly concerning because CISA is responsible for "understand[ing], manag[ing], and reduc[ing] risk to [the United States'] cyber and physical infrastructure."[31] They also provide many security resources to financial institutions including "scans of internet-facing systems to identify vulnerabilities and … confidential, actionable feedback."[32] With CISA's reduced workforce, the agency has less resources to support banks and identify security shortcomings. These cuts may also limit banks' ability to address cyber threat information sharing between the government and the private sector.[33]

---

[24] *Id.*
[25] Federal Deposit Insurance Corporation and Office of the Comptroller of the Currency, Federal Register Notice, "Unsafe or Unsound Practices, Matters Requiring Attention," October 30, 2025, https://www.federalregister.gov/documents/2025/10/30/2025-19711/unsafe-or-unsound-practices-matters-requiring-attention.
[26] Board of Governors of the Federal Reserve Division of Supervision and Regulation, "Updated Statement of Supervisory Operating Principles, April 21, 2026, https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260430.pdf.
[27] Bloomberg, "US Treasury Seeking Access to Anthropic's Mythos to Find Flaws," Margi Murphy and Rachel Metz, April 14, 2026, https://www.bloomberg.com/news/articles/2026-04-14/us-treasury-seeking-access-to-anthropic-s-mythos-to-find-flaws?srnd=homepage-americas; Bloomberg, "Bessent Calls Anthropic's Mythos a Breakthrough in China AI Race," Laura Curtis, April 14, 2026, https://www.bloomberg.com/news/articles/2026-04-15/bessent-calls-anthropic-s-mythos-a-breakthrough-in-china-ai-race.
[28] The New York Times, "Dozens of Government Technology Specialists Fired," Karoun Demirjian and Madeleine Ngo, March 3, 2025, https://www.nytimes.com/2025/03/03/us/politics/18f-technology-specialists-fired.html.
[29] NPR, "The Trump administration admits even more ways DOGE accessed sensitive personal data," Stephen Fowler and Jude Joffe-Block, January 30, 2026, https://www.npr.org/2026/01/23/nx-s1-5684185/doge-data-social-security-privacy.
[30] Cybersecurity Dive, "CISA workforce cut by nearly one-third so far," Eric Geller, June 4, 2025, https://www.cybersecuritydive.com/news/cisa-departures-trump-workforce-purge/749796/.
[31] Cybersecurity & Infrastructure Security Agency, "About CISA," https://www.cisa.gov/about.
[32] Community Banking Connections, "Cybersecurity Risks and Resources," Andrew Pasternak, August 19, 2025, https://www.communitybankingconnections.org/articles/2025/third-release-2025/cybersecurity-risks-and-resources.
[33] Cybersecurity Dive, "CISA's international, industry and academic partnerships slashed," Eric Geller, October 22, 2025, https://www.cybersecuritydive.com/news/cisa-stakeholder-engagement-division-layoffs-critical-infrastructure-international/803433/.

Recent advancements in AI technology have intensified cyber threats to the financial system—especially in light of the development of Mythos— and the Trump Administration should immediately reverse course on its deregulatory agenda, reverse the drastic cuts to the government's cyber resources, and promulgate stronger rules around bank supervision, vulnerability identification and remediation, third party vendor oversight, and threat information sharing. Enhancing these safeguards is necessary to hold financial institutions accountable for protecting consumer data and to ensure resilience against cyberattacks.

In an effort to better understand Treasury's efforts to strengthen the cybersecurity resilience of the financial sector amidst the growing risks of AI-enabled cyberattacks, I request that you respond to the following questions by June 16, 2026:

1. Has Treasury completed an analysis on the root causes of data breaches within financial institutions from January 20, 2025 to present?

    a. Summarize any and all actions you have taken as a result of this analysis.

    b. Describe any necessary updates to legislation that will help alleviate risks caused by these breaches.

2. Describe and summarize any risk assessments Treasury has conducted concerning the "Unsafe or Unsound Practices" proposed rule and its impact on cyber risk management.

3. Explain the extent to which the recent development of Mythos and increasing trends of cybersecurity breaches at financial institutions have impacted Treasury's guidance to the FDIC and OCC regarding its "Unsafe or Unsound Practices" proposed rule.

4. Does Treasury have any plans to coordinate or recommend regulatory or supervisory enhancements to ensure that financial institutions are resilient against the most prevalent cyberattacks, including supply chain attacks, third party vendor vulnerabilities (including cloud service providers), AI-enabled phishing attacks, and skimming? If so, please describe the agency's planned actions.

5. Has Treasury conducted a risk analysis of CISA workforce reductions?

    a. If so, summarize the impact of these reductions on the Department's cybersecurity coordination responsibilities.

    b. Describe actions that Treasury has taken to prevent barriers in communication and coordination between financial institutions and the Federal government.

6. Does Treasury monitor common methods used by banks to monitor security standards and risks associated with third party vendors?

    a. If so, provide data summarizing how frequently banks conduct third party cybersecurity evaluations.

b. Describe efforts that Treasury has made to provide guidance to reduce the concentrated risk of third party vendors.

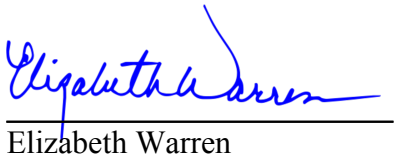
7. Has Treasury evaluated current regulations around the frequency of vulnerability scanning and remediation, penetration testing, and the implementation of bug bounty and vulnerability disclosure programs?

   a. If so, please share Treasury's findings and any plans to update these regulations.

   b. If not, explain.

8. Given Mythos' capabilities of finding and exploiting zero-day vulnerabilities, its impending release to the public, and the potential future release of similar models, what actions has Treasury taken to ensure that financial institutions are resilient against AI-enabled cyberattacks, specifically the increased risk of the exploitation of zero-day vulnerabilities?

Sincerely,



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