

February 4, 2026

Senate Committee on the Judiciary

Senate Committee on Banking, Housing, and Urban Affairs

Re: JP Morgan Chase Managing Director Christy Lillie's protected whistleblower disclosure of egregious mistreatment of customers, \$1.6 billion in dirty money, >\$100 million unpaid fraud claims, Bank Secrecy Act and sanctions violations, unlawful suppression of evidence, and retaliation

I. Introduction

To the Senate Judiciary and Banking Committees:

1. I am a lawyer representing **Christy Lillie**,¹ currently **Head of Scam Prevention** and Managing Director in Consumer and Community Banking ("CCB") at **JPMorgan Chase Bank** ("Chase"). She has worked passionately for years to combat the ongoing epidemic of **frauds and scams**. Unfortunately, my client discovered that Chase has been engaged in extremely serious legal violations which threaten the life savings of millions of Americans. Ms. Lillie worked hard to fix these problems from her senior position within the bank, but at almost every turn she was met with deliberate efforts to deceive regulators. Reluctantly, she became a protected, lawful whistleblower,² after which the Departments of Justice and the Treasury opened investigations. Now, while she is suspended from her job in retaliation for her whistleblowing, Ms. Lillie is making these protected disclosures to Congress,³ and is willing to testify publicly about the devastating impact of Chase's malfeasance on our children, our grandparents, and the American people.
2. When banks fail to stop unauthorized break-ins and thefts from client accounts, U.S. law requires them to reimburse the victims. But over the last several years, Chase has **unlawfully denied over \$100 million** in legally mandatory fraud reimbursements

¹ <https://www.linkedin.com/in/christylillie>.

² Ms. Lillie filed protected disclosures with the Securities and Exchange Commission, the Department of Justice, and the Department of the Treasury, among others.

³ Please be advised that although the undersigned, as counsel, has prepared this disclosure for submission, my client has reviewed its contents, and the positions espoused herein should be considered as her own. Thus, where a factual statement is asserted and does not include a citation to a supporting document or declaration, the source is my client.



NAPIER NETWORK

to customers whose money Chase allowed to be stolen. Perhaps even more shocking, when Chase does manage to identify and close accounts operated by bad actors, it **allows criminals to keep the fruits of their crimes**, sending them a check without first determining whether **Chase had already been notified — by its own customers or by another bank — that victims existed**, or returning the stolen funds to the people from whom they were taken. Larger balances go to “suspense accounts,” where customers cannot access the funds without law enforcement involvement—and which now hold **\$1.6 billion in dirty money**. Even when victims have accounts at Chase, the bank finds it **too burdensome to determine who the money belongs to**. It is simpler for Chase to donate (“escheate”) the money to the State of Ohio, where the bank has its largest office. In other words, even when Chase is holding the victims’ money in hand, most of the elderly and vulnerable people who have lost their life savings to scammers will never get it back. Once the money goes to Ohio, for victims, for all practical purposes, it is gone. Under these circumstances, even the State of Ohio has signaled concern about continuing to receive such volumes of funds.

3. As information technology has greatly accelerated online financial transactions, it has also fueled a massive, illegitimate industry robbing people of their savings. Frauds and scams against American consumers are now at **epidemic levels**⁴, having quadrupled in the last four years and continuing to rise. Media coverage of new scams appears almost daily, and Americans are receiving more spam and scam calls than ever. Each fraud and scam is a **tragic human story of loss**. These victims are elderly people, thinking they were reimbursing an overpayment, who have lost their life savings. They are teenagers **blackmailed over sexual content**, before they commit suicide. They are ordinary people who believed they were speaking to a Chase representative, shared a verification code, and lost money when the hacker called in and tricked Chase into sending a payment. When victims ask for reimbursement, Chase **refuses to even review the call recordings in its own possession that supposedly authorized the payment**. Often, the scammers

⁴ Between 2020 and 2024, FBI statistics show reported U.S. losses more than quadrupled, from about \$3.8 billion to \$16.6 billion, affecting millions of victims. See https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf. The Federal Trade Commission estimates that in 2024 nationwide losses reached \$158 billion, once adjusted for the roughly 75% of fraud that goes unreported—a 25% increase from 2023. See <https://www.ftc.gov/news-events/news/press-releases/2025/03/new-ftc-data-show-big-jump-reported-losses-fraud-12-5-billion-2024>. The Global Anti-Scam Alliance reported \$1 trillion lost to scams worldwide in 2024. See <https://www.gasa.org/post/global-state-of-scams-report-2024-1-trillion-stolen-in-12-months-gasa-feedzai>



NAPIER NETWORK

themselves are literal slaves, forcibly trafficked by organized crime networks to office park call centers in developing countries such as Myanmar.⁵ These human stories have brought Ms. Lillie to tears many times. It is her commitment to stopping the exploitation of vulnerable people that motivates her to come forward now. The exploitation begins with the fraudster, who may trick victims into giving up a security code, and continues when the bank declines the claim, leaving those least able to challenge the decision with no way to get their money back.

4. My client hasn't just had a front-row seat to these tragedies—on many issues, for some of the largest banks in the United States, she has been **the prime mover** driving solutions behind the scenes. Before joining Chase, my client was at Bank of America ("BoA") for more than a decade and left as Head of Digital Payments for the bank. Since moving to Chase in 2021, my client has personally led the firm in beginning to meet some of its fraud reimbursement obligations under the law, implementing better authentication and security in bank call centers, and making many other important changes to help Chase's tens of millions of customers. My client is one of the **handful of global experts** on frauds and scams affecting victims worldwide.
5. In every part of her life, Ms. Lillie puts integrity, and helping others, first. Ms. Lillie and her husband are parents of six children, two of whom they adopted through China's special-needs program. They have also hosted an international foster child for donated medical care, and have provided respite foster care through their church community. Ms. Lillie serves on the board of a nonprofit supporting orphans in China. She brings the same deep concern when trying to stop scams before they happen, and to helping the victims afterwards. For Ms. Lillie, being the Head of Scam Prevention for Chase was her dream job because it meant helping people every day.
6. **Anti-Money Laundering & Sanctions Violations:** After Ms. Lillie started four years ago, her teams began noticing a range of compliance deficiencies across the complex set of laws and regulations governing large banks. While some of the deficiencies were quite serious, they were mostly inadvertent when first discovered. For example, for over 20 years, because of flawed processes, Chase failed to identify fraudsters banking with it, resulting in the **failure to flag tens of thousands of suspicious accounts** for potential closure and **other reporting and controls** required

⁵ See <https://www.bbc.com/news/articles/cw076g5wnr3o>



NAPIER NETWORK

under the anti-money laundering Bank Secrecy Act ("BSA") (and continued to fail at this for a full year after Ms. Lillie's team identified the problem internally). Ms. Lillie has provided lists of thousands of such suspicious transactions to prosecutors at the U.S. Attorney's office for the Southern District of New York. Separately, U.S. national security laws require banks to identify and block transactions involving Specially Designated National persons subject to economic sanctions. But, for years, Chase's systems have been (and as of the date of Ms. Lillie's suspension remained) misconfigured so that the bank is not properly comparing all recipient details in its possession against the sanctions list. Therefore Chase is sending **hundreds, perhaps thousands, of unlawful payments to blocked persons annually**, years after her team flagged the issue, directly undermining U.S. foreign policy. BSA, sanctions and other violations could trigger hundreds of millions of dollars in fines and criminal penalties from U.S. regulators. Ms. Lillie's compliance analysis on violations of the BSA, sanctions, and other laws and documentary evidence can be found enclosed with this letter.⁶

7. **Frauds and Scams:** Even more troubling for Ms. Lillie is Chase's egregious, unlawful betrayal of its customers when it comes to frauds and scams. In fact, banks distinguish these two terms. For Chase and other banks, a **"Fraud" is a term-of-art**, capitalized for the rest of this disclosure, wherein the bad actor accesses the account, and the *bad actor* hits "send" on the money, most often by impersonating Chase employees. Conversely, a **"Scam" is a term-of-art**, capitalized for the rest of this disclosure, wherein the bad actor, on false pretenses, tricks the *victim* into hitting "send," often impersonating federal agencies like the IRS or FBI. Moreover, there are Fraud + Scam and Scam + Fraud combinations, which we will describe more below.
8. U.S. law also distinguishes Frauds and Scams. Generally, banks are required to reimburse their customers who are victims of Frauds (presumably caused by inadequate bank security), but need not reimburse victims of Scams (on the rationale that the Scam victim authorized the transaction, even if under false pretenses). This letter is focused on the myriad ways Chase has failed to protect its customers from Frauds and Scams, let bad actors operate with impunity and profit from their crimes, refused to treat victims with dignity or even according to the law, and then covered it up to regulators. She also has evidence that bank lawyers and

⁶ Enclosed as "2025_10_24 Lillie 38-page Disclosure to Lake Chase."



NAPIER NETWORK

Chase leadership **effected the destruction of research and documents** related to Scam victims.

9. **Abuse of Privilege:** Finally, Ms. Lillie repeatedly saw Chase leaders working to suppress and bury these issues, even unlawfully, rather than addressing them in line with the OCC's Heightened Standards imposed following the 2008 financial crisis. She has evidence that, on multiple occasions, Chase leadership directed staff to **falsify, conceal and/or cover up** material facts to federal regulators and Congress (a felony violation under 18 U.S.C. 1001). She has evidence that bank lawyers abused legal doctrines like attorney-client privilege **in perpetration of crimes and frauds**. In almost every instance of shielding this illegal activity, Chase refused to document the underlying violation in line with post-2008 requirements, further shielding the issue from regulators, the audit committee, the board of directors, and even from their CEO Jamie Dimon. We will not address the complex Attorney-Client Privilege issues in this disclosure, but will do so in a subsequent disclosure.
10. **Lawful Whistleblowing:** My client is making this disclosure reluctantly and as a last resort solely to seek restitution for the bank's many victims. She worked relentlessly for years to fix these problems from the inside. She raised her concerns not just with her peers and the teams that reported to her, but with senior executives, legal staff, compliance leaders, and even the Audit Committee to the Board of Directors. She decided to become a lawful whistleblower after she continued to see certain personnel concealing and covering up material facts from federal regulators. Ms. Lillie and counsel met for hours with the Departments of Justice and the Treasury to discuss these matters.
11. **Retaliation:** On July 28, 2025, after being asked repeatedly to conceal information to a regulator, Ms. Lillie notified her supervisors that she had become a protected, lawful whistleblower. Since then Ms. Lillie has repeatedly requested to meet with senior executives about her concerns. Chase has denied all her requests, conditioning any such meeting on the participation of perpetrators — namely Chase lawyers who had ordered many of the crimes and frauds she was reporting. On October 22, she was placed on involuntary paid administrative leave, where she remains today. On October 24, Ms. Lillie sent an email to Marianne Lake (CEO of Consumer and Community Bank) detailing the violations described here and asking for a meeting with leadership to discuss. On November 5, Chase outside counsel



NAPIER NETWORK

Sarah Bouchard from Morgan Lewis sent a letter enclosed here,⁷ which is remarkable for both the brazenness and emptiness of its threats against a protected whistleblower who has followed every law. Bouchard demanded that Ms. Lillie **"immediately cease"** making protected disclosures:

Ms. Lillie must immediately cease disclosing and transmitting any such information.

12. Bouchard stated the bank's intent to effect **"return or destruction" of the evidence** in Ms. Lillie's possession:

will provide further instruction, including return or destruction of documents and information.

13. And Bouchard baselessly threatened Ms. Lillie with **"fines or imprisonment"** for her lawful whistleblower activities:

Ms. Lillie's letter makes clear that she has violated federal laws and regulations

which provides for fines and imprisonment.

14. **Whistleblower Legal Protections:** In fact, Ms. Lillie is protected under multiple federal laws in disclosing her reasonable belief in potential legal or regulatory violations.

- a. **Sarbanes-Oxley**, 18 U.S.C. § 1514A, protects Ms. Lillie's right to make these disclosures to "any Member of Congress or any committee of Congress" free from retaliation. A wide range of federal laws and regulations⁸ provide her sweeping protections, not least 31 U.S. Code § 5318(g)(3)(A) which states that any bank employee:

that makes a voluntary disclosure of any possible violation of law or regulation to a government agency or makes a disclosure pursuant to this subsection or any other authority...shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of

⁷ Enclosure titled "2025_11_5 Sarah Bouchard Threats"

⁸ See also Dodd-Frank, 15 U.S.C. § 78u-6(h)(1)(A)(iii); and 12 C.F.R. § 21.11(l).



NAPIER NETWORK

such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure. (emphasis added)

- b. **Federal Witness Protections:** As a witness in ongoing federal investigations, Ms. Lillie is protected by 18 U.S. Code § 1513(e), which states that:

Whoever knowingly, with the intent to retaliate, takes any action harmful to any person, including interference with the lawful employment or livelihood of any person, for providing to a law enforcement officer any truthful information relating to the commission or possible commission of any Federal offense, shall be fined under this title or imprisoned not more than 10 years, or both.

- c. These disclosures to Congress enjoy **absolute immunity** from future defamation claims.⁹ In adopting this standard, the D.C. Circuit held that absolute privilege applied even to unsolicited communications preliminary to a Congressional proceeding — even if no formal proceeding ever occurs — so long as:¹⁰

the communicator [can] show that [s]he would not have made the unsolicited statement but for [her] intention to inform the legislative body on a subject properly within its jurisdiction... [and also] the statement must have some relation to the legitimate legislative business to which it is addressed.

15. **Discretionary Redactions:** Ms. Lillie has carefully limited disclosure of internal corporate documents to those relevant and “reasonably necessary”¹¹ to demonstrate Chase’s legal violations. Nevertheless, Ms. Lillie has worked hard to voluntarily redact certain sensitive information from these disclosures:

- a. **PII:** Out of respect for her colleagues, we have sought to remove most of the **Personally-Identifiable Information (“PII”)** from these disclosures except for a few senior executives. Any customer PII has also been redacted.

⁹ “A witness is absolutely privileged to publish defamatory matter as part of a legislative proceeding in which [s]he is testifying or in communications preliminary to the proceeding, if the matter has some relation to the proceeding.” Restatement (Second) of Torts § 590A (1977) (emphasis added).

¹⁰ *Webster v. Sun Co., Inc.*, 731 F.2d 1 at 5 (DC Cir., 1984).

¹¹ Cf. *Cafasso v. General Dynamics C4 Systems, Inc.*, 637 F.3d 1047, 1062 (9th Cir. 2011) (dicta suggesting that relators under the False Claims Act should limit disclosure of internal corporate documents to those documents “reasonably necessary” to pursue their whistleblower claim).



NAPIER NETWORK

- b. **ACP:** We have also redacted materials that are protected by Chase's **Attorney-Client Privilege**. In a separate, subsequent disclosure, we will explain why we reasonably believe the Crime-Fraud Exception to ACP means that some documents marked "Privileged" by Chase may not, in fact, be privileged.
- c. **CSI:** Finally, communications between banks and supervisory agencies like the Office of the Comptroller of the Currency ("OCC") constitute a special class of information called **Confidential Supervisory Information** ("CSI").¹² In general, parties must obtain the permission of the supervisory agency, in this case the OCC, before sharing CSI with any other party. But Article I of the Constitution provides Congress with broad authority to obtain information for legislative purposes, including materials relevant to entities created by Congressional statute such as the OCC. Congress has passed a statute stating that CSI laws shall not "be construed as preventing or limiting access to any [such CSI] information by any duly authorized committee of the Congress."¹³ Whistleblowers may properly provide CSI to Congress, and Congress may properly receive CSI as part of the oversight and legislation process. **Nevertheless, out of deference to any potential ongoing investigations of these matters, we have redacted all CSI from this disclosure and the accompanying materials.**

[Continued next page]

¹² "Non-public OCC information... includes a record created or obtained by the OCC in connection with the OCC's performance of its responsibilities; a report of examination, supervisory correspondence, an investigatory file compiled by the OCC ... in connection with an investigation, and any internal agency memorandum...and confidential information relating to operating and no longer operating national banks." 12 CFR § 4.32(b).

¹³ 12 U.S. Code § 1828b(b)(4).



NAPIER NETWORK

II. In Violation of Law, Chase Leaves Its Customers Holding the Bag for Frauds and Scams

16. **Basic Legal Authorities:** This letter will not provide detailed analysis of the complex laws and regulations governing banks' obligations regarding Frauds and Scams.¹⁴ For those who are interested, an enclosure¹⁵ provides a bit more depth. The most important legal authorities in this area are:

- a. The **Electronic Funds Transfer Act** ("EFTA"), 15 U.S.C § 1693 et seq., is a 1978 federal statute passed initially to regulate Automatic Teller Machines ("ATMs"), setting minimum requirements for banks to investigate and reimburse Frauds, and requirements for consumer-facing Digital Service Agreements. "Wire Transfers" have historically been excluded from coverage and therefore Fraud reimbursement liability, but a recent New York court decision may effectively bring Wires within EFTA's scope.¹⁶
- b. **Regulation E**, 12 C.F.R. Part 1005, is the primary implementing regulation for EFTA, providing detailed guidance on digital payments and reimbursements, including the requirement that banks are liable not just for Frauds where the victims are unilaterally hacked, but also when victims have been negligent with handling of their ATM cards, plus Third-Party Inducement of Credentials ("TPI") Fraud, in which victims are tricked into giving out their credentials.
- c. **Uniform Commercial Code § 4A** ("UCC4A"), passed identically in all 50 states, states that bank security and authentication protocols must be "commercially reasonable," and prohibits **Unfair, Deceptive, or Abusive Acts or Practices** ("UDAAP," also outlawed by federal laws like the Federal Trade Commission Act and Dodd-Frank).

¹⁴ Under EFTA and Regulation E, different federal rules apply to Wire Transfers, versus other types of electronic transfers, versus cash transactions, versus paper checks. Inter-bank Wire Transfers, that are sent across Fedwire, SWIFT or CHIPS networks, require different reimbursement treatment from intra-bank "Wire Transfers", which are processed as "book transfers" within one bank. Some important elements, such as minimum security requirements for online transactions, are governed by state, not federal, laws. The distinction between Frauds and Scams, which is relevant for reimbursement liability, is not relevant for suspicious transactions under the Bank Secrecy Act. Even before the recent wind-down of the CFPB, the alphabet soup of supervisory and enforcement agencies — OCC, FDIC, FinCEN, OFAC, DOJ, FTC, NCUA, FCA, FRB, IRS, OFR, plus state Attorneys General — had rather complex delegations and limitations of authority, overlapping jurisdictions, and parallel-but-independent regulations promulgated from identical statutes.

¹⁵ Enclosed as "2025_10_24 Lillie 38-page Disclosure to Lake Chase."

¹⁶ See *New York v. Citibank, N.A.*, Case No. 24-CV-659, 2025 WL 251302 (S.D.N.Y. Jan. 21, 2025).



NAPIER NETWORK

17. The Fraud and Scam pipeline looks like this: The bad actor exploits weaknesses in Chase's protocols to steal money; the victim discovers the problem and reports it to Chase; Chase is required to perform a reasonable investigation; Chase issues its determination based on policies determined by Chase Legal department; then in some cases, denied victims pursue escalation and/or litigation against Chase. At every step of this pipeline, Chase is breaking the law and treating its customers with disdain.

Before the Crime: Inadequate Phone-Based Authentication Protocols

18. **Chase's "Fraud Hotline" is Inadequate:** Sometimes when a Fraudulent transaction is initiated, Chase's automated systems will flag the transaction as high-risk and slow it down for additional Fraud review. In many instances, the bad actor will proactively contact Chase's "Fraud Hotline" call center to attempt to immediately authorize the transaction before the victim is notified by or has an opportunity to call Chase. Often, the fraudster has the victim on one line while simultaneously working with Chase's Fraud Hotline on another, switching back and forth in real time to obtain the information needed to approve the transaction. Chase's poor Fraud Hotline phone-based security and authentication protocols often are the source of the Fraud itself, reflecting the bank's refusal to protect — even its callous disregard for — its own customers.

19. Examples of these security gaps over the past few years, some of which have not been remediated even after my client and other Chase employees identified compliance gaps years ago, include:

- a. **Fraudster Authentication Bypass ability:** If a Fraudster calls to "validate" a payment but does not like the authentication method demanded by the Chase associate (e.g. "what is your debit PIN and CVV?") they can ask to "bypass" this authentication method to try another ("let me send you a One-Time Passcode"). Chase gives Fraudsters many options to "authenticate."
- b. **Knowledge-Based Authentication (KBA):** A bad actor can, by claiming to have lost their phone, bypass standard authentication and need only answer multiple-choice questions such as "Which of the following addresses have you lived at?" Almost all of these answers are easily accessible to Fraudsters through public records or websites. Regulatory and standards bodies, including