

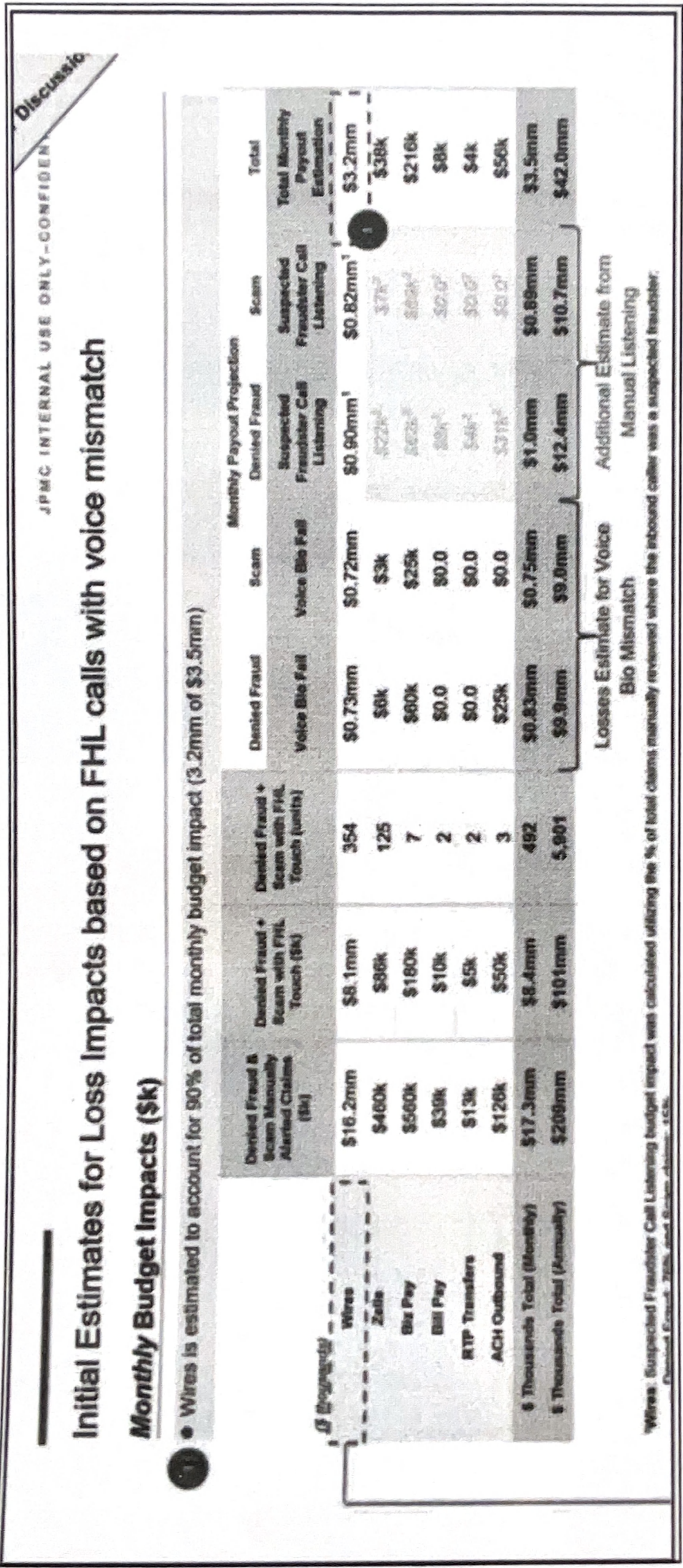


Figure 1



NAPIER NETWORK

41. Unreasonable Determinations of "Reasonableness": Over the past two years, the firm has routinely denied valid EFTA claims without fully utilizing all available internal and vendor data. When questioned on these matters, the Claims team frequently argues that using certain internal or vendor data is "not reasonable" in their opinion. For example:

- a. **Victims don't get the best tools:** In fraud prevention, teams continually update technology, including services from data vendors, to ensure they have the strongest data on SIM porting to other devices, to limit the bank's exposure. When Chase's money is on the line, the bank utilizes both Neustar (a TransUnion company) alongside LexisNexis, to provide the most coverage and best detect SIM porting and prevent fraud. But, in reimbursement cases, Chase only uses LexisNexis for client Fraud claim investigations. Moreover, Chase reimbursement department has configured LexisNexis to detect SIM porting activity (SIM-swaps to redirect One Time Passcodes) only within the past 120 days, despite the fact that the other departments at the bank utilize LexisNexis to review SIM porting events for longer time periods. SIM-porting events can demonstrate Fraud (in which the bad actor began receiving SMS codes intended for the victim's phone), but if Chase doesn't know they occur, the firm simply denies the claim, assuming the client must be lying when they say they did not get a code.
- b. **Technical Data Ignored:** In many cases, significant technical data (e.g. device ID, IP address) exists within the firm's databases; however, Chase's reimbursement department only utilizes this information to reimburse requests submitted within the past 12 months. They do this, not due to regulatory constraints, but because the investment required to pull data between 12-24 months out of Chase's central database and to the Chase associate-facing system has been deemed too costly.
- c. **Malware Ignored:** Malware is malicious software that can infect a customer's computer or phone and allow a fraudster to operate the device remotely, capture credentials, or initiate transactions without the customer's knowledge. **During Chase's claims reimbursement process,** if the authorizing device (the one that sent the payment) is "known to Chase" (e.g. logged in previously), Chase will likely deny reimbursement claims — even if a customer reports obvious signs of malware like pop-ups, fake tech-support calls, or clicking on



NAPIER NETWORK

suspicious links. Even after the decline, victims are never told they likely still have malware on their computer (potentially enabling future thefts), or that malware could have been the source of the payment and could be proven with a letter from a third-party technician like Geek Squad. Only if the victim appeals the denial, and knows to include proof of malware, will Chase reimburse the claim. By withholding this information from victims, Chase is strategically disadvantaging the most vulnerable victims, often older adults, limited-English speakers, and less tech-savvy individuals who are least able to articulate to Chase what occurred and/or navigate these logistical hurdles to get their claims approved.

- d. **Forced EFT Initiation:** Robbery of an access device (e.g. a debit card) and/or forced initiation of a cash withdrawal at an ATM is covered under EFTA, and these claims are paid by Chase when the company has the facts. However, that same analysis is not always applied to non-cash transactions, including electronic transfers conducted through Zelle. This has occurred because claims did not historically request or document the information from the victim necessary to evaluate whether the customer acted under duress, or because coercion is treated as insufficient unless it satisfies an extremely narrow or literal standard — for example, a demand for proof that a weapon was actually held to the customer's head. As a result, most electronic transactions carried out under physical threat are mischaracterized as "authorized."

42. **No Call-Backs or Followup:** Chase's claims investigators do not typically call back the victim to ask questions or get more details on what occurred. Instead, these investigators typically rely on the information provided to them from the call center agent that took the inbound call/claim from the victim. This restriction means that once a claim is filed, as a practical matter, the investigator decides based only on the information provided in the initial report. Without the ability to clarify inconsistencies, probe for context, or confirm details, the process is stacked in favor of quick denials based on incomplete data. This structure is strategic for Chase, as it reduces "claim handle time," resulting in decisions being made more quickly, albeit with less information. In those circumstances, it becomes easier to reach outcomes that deny reimbursement, even where additional inquiry might have supported the customer's claim.



NAPIER NETWORK

43. **No Audit Trail:** When Chase denies a claim, its internal systems do not require — or even allow — a standardized reason code for the denial. Instead, decisions are documented only in free-form associate notes, which may or may not reflect the actual procedures in effect at the time. For auditors, this creates a nearly impossible task: combing through scattered notes and changing processes to determine whether regulations and/or procedures were followed, with no reliable categories to track patterns or test compliance at scale. By design, this system makes denials difficult to re-review, minimizes accountability, and obstructs any meaningful oversight. As a result, for example, in 2023, only **one single Zelle claim** was audited by JPM Chase Fraud Operations Audit team, this in a year that multiple Zelle lawsuits asserted gaps in fraud and claims reimbursement practices, and the same year in which Chase faced about ten thousand arbitrations on this kind of issue. Moreover, even when Ms. Lillie or her team identified compliance gaps; those issues were not entered into Chase's mandatory internal compliance tracking system, known as CORE, which is required to provide visibility to regulators, senior leadership, and the audit committee, further preventing the ability for effective audit oversight, thereby preventing any ability to conduct effective oversight.

[Continued next page]



NAPIER NETWORK

IV. Unlawful Claim Reimbursement and Notice Policies

44. **Unlawful Refusal to Reimburse Fraud + Scam:** In Fraud + Scam cases, despite clear applicability of EFTA to the initial internal Fraud transfers from the Brokerage deposit account, Chase simply ignores the initial Fraud reimbursement claim, and accepts a claim only on the second payment, which they reject on the grounds that the victim authorized it. Shockingly, even when a claim is opened for this fraudulent transfer to the checking account, reimbursement may be denied on the basis that the customer is said to have “received a benefit” from the transaction. We have enclosed a transcript²⁵ of a recording of Ms. Lillie and other staff listening and discussing audio recording of a victim trying to explain such a situation to Chase claims, and Chase failing to open the Internal Funds claim as required by EFTA.
45. **Unlawful Refusal to Reimburse Scam + Fraud:** Again, Chase considers the initial Scam to wipe away the later Fraud in which Chase systems were compromised, and denies all such claims without investigation, in violation of EFTA, reasoning that Scam victims have only themselves to blame. Chase’s Voice Bio and call-listening “Scams + Fraud” metrics described above suggest the exposure may fall in the range of \$10–\$20 million annually. Chase’s practice of automatically declining such claims—without even researching the second step of authentication via voice—is a violation of EFTA or, in the case of Wires excluded from EFTA, the Uniform Commercial Code. Both legal regimes require the bank to treat these transactions as “unauthorized,” and require reimbursement. From the *Widow Victim 1 v. JPMorgan Chase* arbitrator decision:²⁶

²⁵ Enclosed as “2024_10_14 Victim Customer Service Call Claim Not Taken.” My client has audio of the conversation about the customer call; the customer call itself can be subpoenaed from Chase.

²⁶ Enclosed in Redacted Chase Documents.



NAPIER NETWORK

18 The most persuasive case on the issue appears to be Green v. Capital One, N.A. 557 F.
19 Supp. 3d 441 (S.D.N.Y. 2021), a trial level EFTA case tackling the same “authorized” issue
20 presented on this Commercial Code claim, and involving very similar facts. In Green, Plaintiff
21 unwittingly gave an impersonating scammer some of the bank account information sought, and
22 significant sums were transferred from his account without consent. A main issue was the same
23 as here in Ms. [REDACTED] case: Capital One argued that the transfers were not “unauthorized,” but
24 were actually “authorized” because Green voluntarily provided his personal and account
25 information to the scammer, giving the “means of access” to the account.
26
27

1 The Board of Governors of the Federal Reserve System, and separately the Consumer
2 Financial Protection Bureau had each promulgated supplementing regulations. Both
3 interpretations include a fraud clarification that an “unauthorized” transfer includes a transfer
4 initiated by a person obtaining access through fraud.
5
6 The Green court rejected Capital One’s argument. First, it found that access to account
7 information furnished in the first instance under fraudulent pretenses is not “authorized” access.
8 Second, and separate from the fraud clarification, the court held that the transfer “would
9 otherwise be considered ‘unauthorized’ under a common sense understanding of the word.”
10 The Court noted that “access obtained by fraud was never truly ‘authorized.’”
11
12 Although there is apparently no formal clarification for this part of California’s
13 Commercial Code, there doesn’t need to be. It is a matter of common sense. There appears to
14 be no valid reason why the reasoning in Green should not apply here. The re-definition of the
15 “unauthorized” concept is inventive, but unnatural. As Green observed, account access
16 information furnished in the first instance under fraudulent pretenses is, by its very nature, not
17 authorized; it is common sense that a transfer obtained by fraud is not truly “authorized.”
18



NAPIER NETWORK

46. **Unlawful Digital Services Agreement ("DSA"):** EFTA makes Chase responsible for reimbursing Frauds (bad actor hits "send") but not Scams (victim tricked into tapping "send" on false pretenses), and prohibits banks from shifting this liability onto victims via contracts.²⁷ Nevertheless, Chase's current **Digital Services Agreement (DSA)**²⁸ has for years, in various formulations, indicated that negligent handling of a user ID or password can result in customer liability. In the current DSA, this concept appears in several notable provisions: (1) if a customer *"make[s] information available to persons that would enable them to create a Password for and/or access your accounts ... you are responsible for the Bill Payments and/or Transfers they complete. You make information available when you provide it and/or fail to secure it."* (2) *"Our guarantee does not cover losses which you cause.. such as ... your negligent handling of User IDs and passwords."* (3) users *"agree to indemnify and hold us and our officers, directors, employees, and agents harmless from and against any loss, damage, liability, cost, or expense of any kind ... in relation to ... use of the Service by anyone using your Card number, account number, PIN, user ID, or Password"*. This language appears inconsistent with the liability framework of the Electronic Fund Transfer Act, particularly where bad actors — often posing as bank representatives — obtain personal information or credentials through deception because the statute does not treat consumer negligence, by itself, as determinative of authorization. Such messaging overstates consumer responsibility relative to the statute and reasonably leads customers to believe they possess fewer protections than the law affords, raising potential concerns under Unfair, Deceptive, Abusive Acts & Practices ("UDAAP") under the Uniform Commercial Code and federal law. My client has raised these concerns with the drafters of the DSA on multiple occasions, yet variations of the same negligence-based language remain in place, reinforcing her assumption that the messaging is strategically deceptive, in a manner similar to the "Banks Never Ask That" campaign.

47. **An estimated \$68 Million in Unlawful Third-Party Inducement of Credentials ("TPI") Fraud Reimbursement Denials:** The EFTA defines "unauthorized electronic funds

²⁷ See 15 U.S.C. §1693g and 12 CFR §1005.6.

²⁸ Available at

https://static.chasecdn.com/content/dam/legal-agreements/library/en/dsa1_la/versions/dsa1_la.pdf



NAPIER NETWORK

transfer" (what banks call Frauds, which require investigation and reimbursement) as:²⁹

an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit... (emphasis added)

48. Scams (in which the victim hits "send") have in practice been excluded from this definition of TPI Fraud because they are not "initiated by a person other than the consumer." The statutory definition of "unauthorized" EFTs obviously includes situations where Fraudsters unilaterally steal debit cards from their wallets, hack victims' passwords, or put malware on their laptops. In many other cases, victims did not initiate the transaction, but in some way, inadvertently, assisted the bad actor. For example, perhaps they forgot their wallet in a public place, from which their debit card was taken. Or, believing they are speaking to a Chase representative, victims hand out their SMS One-Time Passcode (called **Third-Party Inducement of Credentials or "TPI"**).
49. For decades, Chase simply refused to pay TPI reimbursement claims (e.g. where the client did not hit 'send' but was tricked to give out a code), arguing that the victim is to blame for their own loss. But a straightforward reading of the statutory text affirms that when victims are tricked, even if they were negligent with their credentials, the transaction was nevertheless "unauthorized" and subject to reimbursement because it was "initiated by a person other than the consumer without actual authority to initiate such transfer..." Simply because victims were negligent in handling their credentials does not mean they ever authorized the Fraudulent transaction.
50. For this reason, US Banks including **Wells Fargo, Bank of America, Capital One and since 2021, Chase, all acknowledge they are required to pay TPI** reimbursement claims for Electronic Fund Transfers. Intuitively, it makes sense that banks bear liability for these Frauds, because it is the banks that create the applicable security and authentication protocols which customers are forced to rely on.

²⁹ 15 U.S. Code § 1693a(12).



NAPIER NETWORK

51. This issue of EFTA compliance has recently drawn the attention of the Senate Banking Committee, the New York Attorney General³⁰, and many consumer advocate groups. Wire transfers are a key point of concern. The EFTA contains an exclusion when a Wire is processed through a network system such as Fedwire or CHIPS. However, when both the sender and the recipient hold accounts at the same institution, large banks often do not use those networks to process the wire. Instead, they complete the transaction internally as a book transfer—a ledger entry that avoids sending the payment through an external system. Because these transfers do not pass through the networks that trigger the exclusion, the EFTA applies. That is why institutions such as Wells Fargo, Capital One, and Bank of America evaluate reimbursement claims arising from these internal book transfers under the EFTA framework. Chase, by contrast, did not do so for decades, declining millions every month unjustly.
52. In addition to Wires, over many years and many products, and still today for important products, Chase has unlawfully refused to reimburse TPI fraud claims. Before she was suspended, my client used internal bank data to estimate that since agency guidance clarified TPI liability in June 2021,³¹ Chase has **unlawfully declined approximately \$68 million in valid TPI Fraud** reimbursement claims across four payment rails. In each of these cases, the full-time lawyers, compliance, risk, controls and supposed subject-matter experts who had been overseeing the reimbursement process for years had either not noticed the EFTA violations, or simply decided they did not want to pay them.³²

³⁰ See *New York v. Citibank, N.A.*, Case No. 24-CV-659, 2025 WL 251302 (S.D.N.Y. Jan. 21, 2025, holding for apparently the first time that Wires are covered by EFTA; this ruling is currently on appeal to the Second Circuit). Historically, while EFTA mandated reimbursement for non-Wire digital payments, Wire Frauds were covered under the Uniform Commercial Code, which was more favorable to banks. This discrepancy meant that whether the loss was borne by the victim or the bank depended on whether the bad actor decided to steal money using a Wire Service, or a non-Wire service like Zelle.

³¹ 2021 agency guidance states:

A third party fraudulently induces a consumer into sharing account access information that is used to initiate an EFT from the consumer's account. Does the transfer meet Regulation E's definition of an unauthorized EFT? Yes.

Available at

<https://www.consumerfinance.gov/compliance/compliance-resources/deposit-accounts-resources/electronic-fund-transfers/electronic-fund-transfers-faqs/>.

³² Chase internal documents referencing the detailed figures mentioned here can be found in the extensive, redacted Chase documentation enclosed.



NAPIER NETWORK

- a. **Zelle** (TPI claims unpaid until October 2021). Chase's internal data show approximately \$800,000 in paid Zelle TPI claims in October 2021; if representative, that would suggest roughly \$3.2 million in previously unpaid claims over the preceding four months following issuance of applicable regulatory guidance.
- b. **Bill Pay Checks** (TPI claims unpaid until September 2023, almost a full year after my client flagged the issue). Chase's internal financial analysis estimated approximately \$3.6 million in Bill Pay checks TPI exposure for the first year after reimbursement practices changed. Using that figure as a proxy, and applying a conservative downward adjustment to account for growth in fraud in later periods, my client estimates unreimbursed claims from June 2021 through October 2023 at approximately \$7 million across the 28-month delay from regulatory clarification to Chase's implementation.
- c. **Interbank Wires (Fedwire/Chips) and Chase-to-Chase Book Transfer Wires** (TPI claims unpaid until June 2024, two full years after Ms. Lillie notified Chase of the compliance deficiency). Internal data indicates that roughly \$3–4 million per month in TPI wire and book-transfer claims were being declined just prior to the process change implemented in June 2024. Using that figure as a proxy, and conservatively adjusting downward to account for increasing fraud trends during the three-year period, my client estimates approximately \$58 million in unreimbursed TPI wire and book-transfer claims between June 2021 and June 2024.³³
- d. Ongoing violations of unpaid TPI Fraud claims for **Brokerage Deposit Sweep accounts** (Ms. Lillie identified this gap in June 2025, which is still not repaired). JPMorgan Chase treats the deposit account tied to the Self-Directed Investment (SDI) account as ineligible for EFTA coverage, despite the fact that the linked sweep deposit account is for personal use, FDIC-insured, interest-bearing, and supports electronic fund transfers (EFTs) such as ACH transfers and check deposits. As a result, Chase fails to apply core EFTA protections for unauthorized transactions—including refusing to accept claims

³³ This estimate includes both interbank wires transmitted over networks such as Fedwire and CHIPS and intrabank book transfers that were presented to customers as wires, as consumers could not reasonably be expected to distinguish between these mechanisms when reporting the fraud, creating a requirement of consistent treatment.