



NAPIER NETWORK

the National Institute of Standards and Technology (NIST) and the Federal Financial Institutions Examination Council (FFIEC), began warning as early as 2017 that this method was insecure. Chase would allow such authentication to send a \$50,000 wire out of a clients account.

- c. **Repeated Failures Not Flagged or Blocked:** Then, when Fraudsters nevertheless fail authentication, Chase neither locks the account nor notifies the account holder of the ***repeated authentication failures***. Chase lets the Fraudsters keep trying. If the multiple choice question has five possible answers, the Fraudster could have called in five times till they answer correctly.
- d. **No Declination Authority:** Even when it is obvious that the caller is a Fraudster — for example, a young male voice pretending to be an elderly female client — Chase call center associates are prohibited from declining authorization so long as the caller successfully completes the inadequate “authentication.” Ms. Lillie has heard recordings of such calls in which, after each question, the Fraudster will literally put the Chase Fraud Hotline associate on hold to switch back to the victim and get the required information. This policy has been in place for years, and though Ms. Lillie pushed hard to change it, it was still happening when Ms. Lillie was put on leave.
- e. **Voice Bio:** Chase Fraud Hotline call center uses Voice Biometric (“Voice Bio”) technology that reviews and blocks some pending transactions before execution if the voice that called in to authenticate the payment did not match the voice Chase has on file. But this indicator of a “voice bio mismatch” was not used in reimbursement claim disputes as an indicator to approve a customer’s claim of fraud.
- f. **No Alternatives to SMS Codes:** JPM Chase has determined that easily-stolen SMS codes are too risky for associates to use to reset their email user name and password; however, they also determined that these text based SMS codes are adequate for protecting their clients’ life savings. This contradiction speaks for itself. SMS codes can be re-routed to Fraudsters through SIM-swapping, or simply requested via phone call to the victim. Obvious and better alternatives used by other major companies include soft tokens / authenticator apps (available to Facebook users), and hardware tokens like Yubikeys and Titan



NAPIER NETWORK

Keys (available to Apple and Google users). **Said another way, Facebook is protecting your vacation pictures better than Chase is protecting your life savings.** To be clear, Chase has secure soft token technology available - they are required for its own staff - but they have not yet offered it to consumers, citing cost and user friction. For the years that Chase was unlawfully declining reimbursement claims following stolen SMS codes, the bank simply had no financial incentive to upgrade security options. This might change following Ms. Lillie's successful efforts to make Chase pay more reimbursement claims for stolen SMS codes.

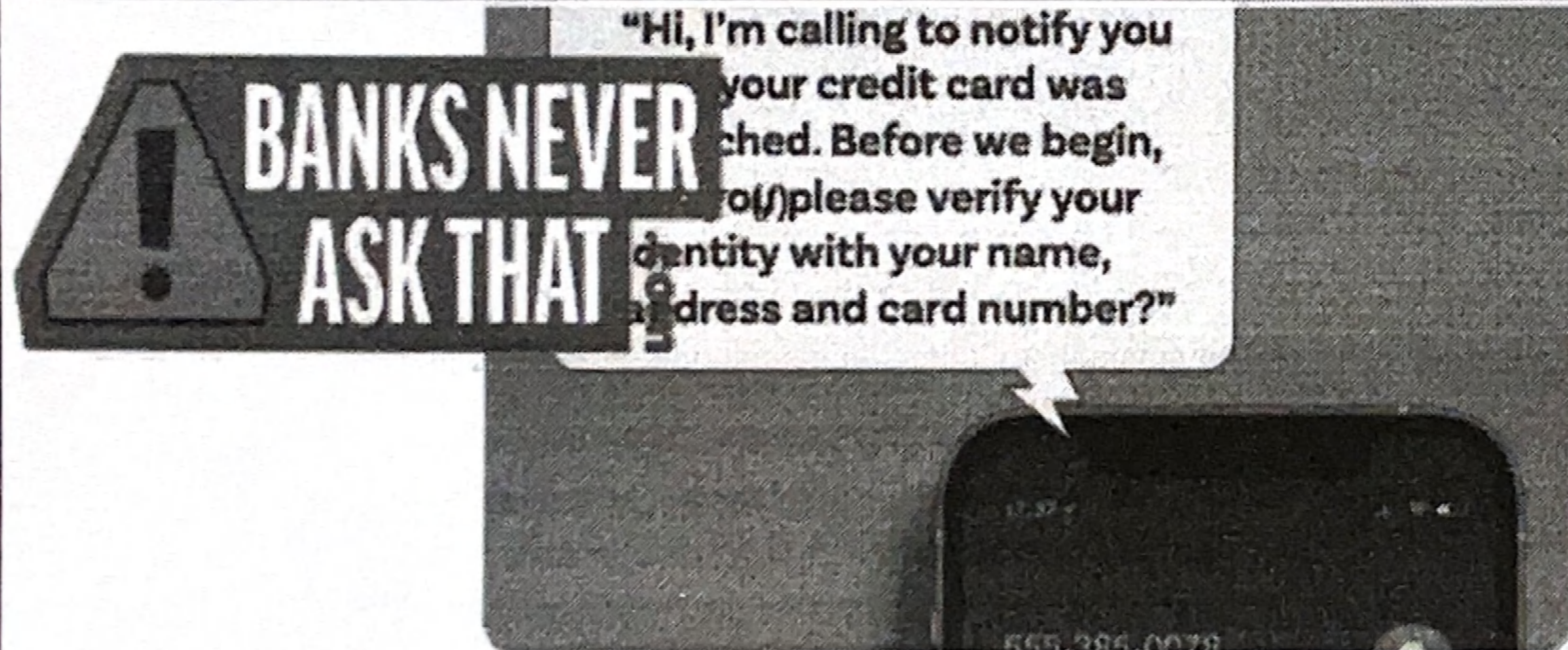
20. Ms. Lillie has **personally heard disturbing recordings** of Chase call center associates speaking with obvious fraudsters. In these calls, the fraudsters often pause after authentication questions - asking the associate to repeat the various multiple choice answers while a second accomplice is on the line with the client obtaining the information requested by the Chase employee. These disturbing calls become devastating when the Fraud is successful, the victim loses their money, and then files a claim for reimbursement, which Chase declines because the caller completed "authorization." Congress is able to subpoena these recordings which are saved in Chase's "Webstat" system. The following Call IDs are worth listening to: 13646790801 and 13647295033 (Fraud Zelle cases); 17088412901 (Large Loss ACH Payroll case); 16073985993 and 10769442397 (Large Loss Wire cases).
21. Some or all of these deficiencies likely represent commercially unreasonable security procedures prohibited under Uniform Commercial Code § 4A. Note that these failures are especially harmful to clients because Chase then routinely unlawfully denies reimbursement for Fraud and Scam losses on the grounds that the caller and the transaction was supposedly "authorized," though in many cases **the bad actor completed authentication. A customer cannot authorize a payment they do not know is being made.** Where the underlying authentication protocols are so weak, such reimbursement denials are not only unconscionable, they raise serious questions under UCC § 4A, which requires security procedures and related determinations to be commercially reasonable.

ABA: "Banks Never Ask That" — but Chase Does.

22. Chase is one of the largest funders of the American Bankers Association ("ABA"), and its ongoing marketing campaign called "Banks Never Ask That."¹⁷ The campaign is presented as an effort to combat Fraud and Scams. However, the campaign's central message — including the statement that banks will never ask for a one-time login code — is simply false. This marketing messaging sits alongside industry practices in which customers are, in fact, contacted by Chase and asked to provide authentication codes.

23. This type of message results in **victim blaming**, leaving customers believing that, if they shared a code, the loss must be their fault and a claim asking for reimbursement (or pursuing escalation on a declined claim) would be futile. **When prevention messaging and real-world practice diverge, confused customers are the ones who bear the consequences.**

24. The website states that "Banks...will never ask for a one-time login code."

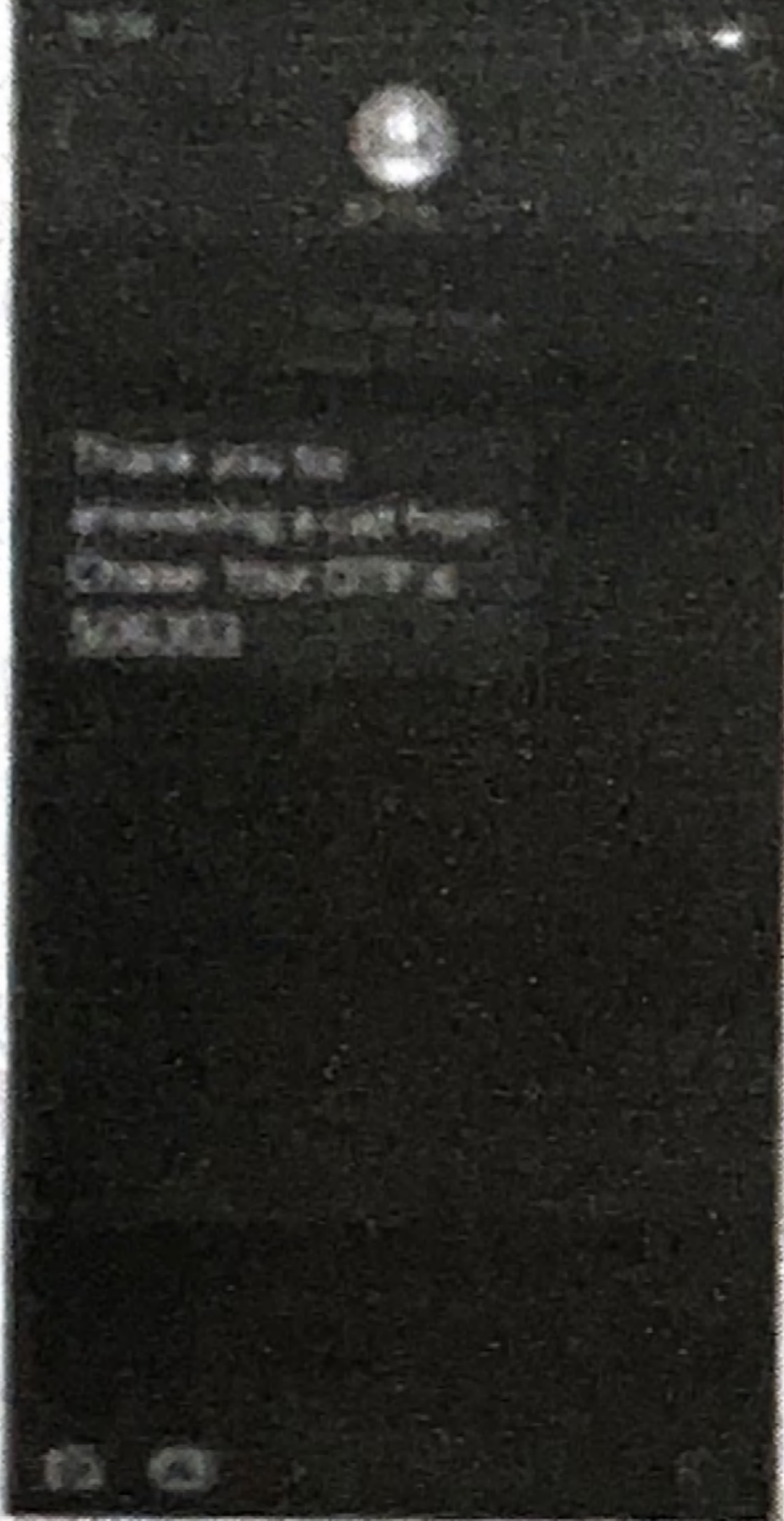


- **Unusual Caller ID**
While caller ID can be spoofed, legitimate calls from your bank are more likely to display an official phone number or a known identifier. If not, be very skeptical.
- **Scare Tactics or Threats**
Phishing calls rely on a sense of urgency. If the caller pressures you into immediate action or threatens negative consequences, just hang up and call the number on the back of your bank card.
- **Asking for Personal Information**
Banks will rarely ask for your account number, PIN, or password during a phone call — and will never ask for a one-time login code. Never share such confidential details unless you've called the number on the back of your bank card.

25. But this is now, and has been for the past 5 years, **quite simply false**. Hundreds of times every day, Chase calls its customers on their mobile numbers, then sends them a One-Time Passcode to the same number and asks them to read it back, supposedly to "verify" them. First, this supposed security procedure does nothing to

¹⁷ See <https://BanksNeverAskThat.com>.

improve security, because the code is sent to the same phone that Chase just called. Second, this procedure — calling a customer, then asking for a code that just arrived — perfectly mimics the technique used by many criminals to gain access to one-time passcodes. Here are the text messages that a Chase client would receive when Chase legitimately calls them to verify a credit card or digital payment:

Outbound Call - EMM	Outbound - First Watch
	
Use Case: EMM will contact a customer in their system queue to verify a pending wire transaction. OTP is used as part of their authentication, since wires are considered high risk. They use OTP in conjunction with ART.	Use Case: Fraud Prevention Outbound will contact a customer in their system queue to verify potential fraud transactions, either monetary or non-monetary. OTP is used as part of their authentication, since fraud call centers are considered high risk.
Current Message: <i>Thank you for answering a call from Chase.</i> <i>Your OTP is 123456</i>	Current Message: <i>Thank you for answering a call from Chase.</i> <i>Your OTP is 123456</i>



NAPIER NETWORK

26. The most common such Fraud purports to come from a Credit Card fraud department. The Fraudster spoofs Chase's call center number, so it looks like Chase is calling them. The fraudster then repeats the script that Chase has as referenced above. The Fraudster uses Chase's website to send a code to the victim, and the code the client gets is actually from Chase — so the ruse is identical to what Chase is actually doing hundreds, if not thousands, of times a day. Then, when a client files a reimbursement claim and admits they gave out a code to the Fraudster, Chase declines the claim recasting the theft as an "authorized payment" and blaming the victim for their "negligence."
27. The ABA campaign also states, falsely, that banks will never call you and ask for personal details.¹⁸

Never give sensitive information

Never share sensitive information like your bank password, PIN, or a one-time login code with someone who calls you unexpectedly — even if they say they're from your bank. Banks may need to verify personal information if you call them, but never the other way around.

28. But Chase's Fraud Hotline call centers, and branches, make outbound calls attempting to authenticate customers or verify suspicious transactions, in which **they ask for "personal information."** Insecure and publicly available "knowledge-based" questions might include "Which of the following addresses did you live at?"
29. **Blaming the Victim:** The disconnect between Chase-funded ABA messaging on giving out these codes, and the reality of what Chase does, is staggering. While the Chase-funded ABA campaign warns and admonishes clients never to give out passcodes or personal details, Chase itself is calling those customers and requiring passcodes and personal details to authenticate, in ways that exactly mimic

¹⁸ See <https://www.banksneveraskthat.com/en/protect-yourself>



NAPIER NETWORK

scammers. Then after victims file reimbursement fraud claims, Chase perversely denies valid reimbursement on the grounds that the victim “authorized” it, and clients supposedly should have known not to give out passcodes or personal details to a caller claiming to be from Chase.

30. It is likely that, as a legal matter, the false ABA campaign language — which has been live online and on billboards around the country for over five years — can be attributed to one of its largest funders, Chase, triggering Unfair & Deceptive Trade Practices violations under the Uniform Commercial Code and Federal Trade Commission Act.
31. Moreover, in 2024, my client personally informed the American Bankers Association during a telephone call with a senior representative — an individual who has previously testified before Congress — that the campaign messaging was inaccurate. Despite that notice, the ABA has continued to disseminate the same representations, even after being informed that they are inaccurate and operate to blame victims. My client further understands that many member banks continue to employ authentication practices inconsistent with the campaign’s claims, raising substantial questions as to whether the ABA verified the accuracy of those marketing statements with the institutions it represents.

[Continued next page]



NAPIER NETWORK

III. Unfair and Unlawful Claim Investigations

32. **Shallow Investigations, Easier Denials:** After victims discover they have been defrauded, they file EFTA claims with Chase. But Chase's EFTA Claim department investigations are structured in ways to make denials easier, leaving customers at a systemic disadvantage.
33. **Refusal to Perform Required Investigations:** While other banks take and review claims from clients up to seven years old (mirroring audit standards requiring seven-year document holds), Chase has adopted a practice of initially outright denying all claims older than 24 months without any EFTA investigation whatsoever, instead forcing victims to return and escalate the decision. After this burdensome process, nevertheless, 13% of the original set of declined cases are ultimately paid, highlighting the injustice of the original decision to decline them. Notably, these types of claims disproportionately impact vulnerable clients, such as elderly individuals who may only later recognize that they have been victims of fraud or abuse, often by caregivers or trusted individuals.
34. **Refusal to Examine Their Own Data:** When conducting an Error Resolution Investigation, a financial institution "must determine whether an error has occurred,"¹⁹ and in so doing, must conduct, at a minimum, a "review of its own records regarding [the] alleged error."²⁰ This review must include "any relevant information within the institution's own records,"²¹ and the investigation "must be reasonable."²² In conducting EFTA investigations for Fraud claims, banks must conduct at least "review of its own records."²³ But Chase regularly and unlawfully declines Fraud reimbursement claims without reviewing even the evidence in Chase's own possession, which often would prove the transaction was not authorized.
35. **Call Recordings:** One example of this data that is not utilized is the call recording of the authorization of the payment itself. Often, Fraudsters call the Fraud Hotline Center and successfully impersonate the victim, and the payment is sent. When the

¹⁹ 15 U.S.C. § 1693f.

²⁰ 12 C.F.R. § 1005.11(c)(4).

²¹ 12 C.F.R. Pt. 1005, Supp. I, Comment 11(c)(4)-5.

²² 71 Fed. Reg. 1638, 1654 (Jan. 10, 2006). In 2019, USAA Bank reached a consent order with federal investigators on precisely these requirements. See

https://files.consumerfinance.gov/f/documents/bcfr_usaa-federal-savings-bank-consent-order.pdf.

²³ 12 CFR § 1005.11(c)(4).



NAPIER NETWORK

victim later files a claim with Chase stating that the transaction was unauthorized, Chase simply denies the claim on the grounds that the Fraud Center received a call that authorized the transaction. Chase does not listen to the call recording, which would prove that the victim (who filed the claim) is not the person who called in to authorize the payment. Chase thinks it would take too long to listen to the voice recordings during its reimbursement claim process. Chase tries to justify this by saying that EFTA does not require the bank to use "all" of its records, merely "reasonable" records, and that Chase gets to decide which records are "reasonable" to utilize. This issue was noted (unfavorably for Chase) by the arbitrator in *[Widow Victim 1] vs. JPM Chase Bank, N.A.; JAMS Ref Redacted* (June 2024).²⁴

3	Chase stopped its verification inquiry at this point. There were additional simple
4	inquires that Chase could have made which would likely have immediately revealed the scam
5	and prevented Ms. [REDACTED] loss. Chase could have called "Barbara" or Ms. [REDACTED] into the
6	nearby branch for a personal interview. Voice comparison was available, but wasn't used, and
7	
8	the difference in voices is apparent to the layman listener even without special equipment.

36. Refusal to examine "Voice Bio" score: For many customers, Chase employs a third-party "Voice Bio" technology to tell the Chase representative whether the voice on the phone matches the voice of the actual client. But the technology is new and imperfect, and when Chase representatives receive a "fail" score, historically, that has not stopped the transaction. Rather, Chase merely falls back to a different, often insecure, authentication method such as the previously described insecure multiple-choice "knowledge" questions. Most concerning, when victims file claims for unauthorized transactions, Chase has not examined the Voice Bio score from the authentication conversation, when often that Voice Bio score would show that the voice on the phone was not that of the victim, indicating that the payment was unauthorized. At Ms. Lillie's insistence, since November 2024, the firm has incorporated Voice Bio mismatch markers in more Wire transfer claim investigations — which is a positive move — improving the bank's reimbursement claim rate for wires. However, gaps remain, and, as of the time my client was put on leave, the EFTA reimbursement claims review process still did not utilize the Voice Bio

²⁴ Enclosed in Chase Redacted Documents.



NAPIER NETWORK

mismatch markers available within Chase systems for payments such as Zelle, Bill Pay, and ACH. Given the technology is a simple score, it appears "reasonable" to incorporate it into Chase's reimbursement claims decisioning.

37. **Fraud + Scam:** During or after the Claims investigation, Chase employs unlawful policies to exclude a wide range of valid claims from coverage. Surprisingly often, bad actors engage first in Frauds (where they break into accounts and hit "send" on internal bank transfers, for which Chase has EFTA reimbursement liability) before Scams (when the bad actor convinces the victim to hit "send" on a payment out, under false pretenses, for which Chase does not have liability under EFTA). For example, perhaps a bad actor can get online account access to transfer \$100,000 from a victim's brokerage deposit account into their checking account, but the bad actor cannot authenticate a wire transfer of this size out of Chase. Instead, the bad actor will call the victim on the phone, point out their unexpectedly large checking account balance, and give the victim a story about how the bad actor (posing as Chase bank or another legitimate institution) "accidentally" deposited money to the victim's checking account. Often, the victim does not notice that their brokerage deposit (held in a different section of the website/mobile app) account now has an equally large debit. Thinking they are a Good Samaritan, the victim agrees to wire back the "mistaken" transaction. In fact, they are sending the bad actor their own money.
38. **Scam + Fraud:** Sometimes, conversely, Scams precede Frauds. For example, in the initial Scam, a victim is tricked under false pretenses to hit "send" on a wire out to a bad actor. But, Chase's automated fraud and scam systems sometimes flag and hold the transaction for review. Then, before Chase's Fraud Hotline can call the Scam victim (where they would ask them for a one time code, in violation of the 'ABA Banks Never Ask That campaign'), the bad actor proactively calls into the Chase Fraud Hotline to authenticate the transaction. By this point, the transaction has been stopped, and it is only re-started because the bad actor is able to "authenticate" as the victim, using social engineering or some other Fraud to obtain information like a one time code or a debit pin. These unauthorized transactions cannot ultimately proceed without the bad actor conducting a Fraud, for which EFTA assigns liability to Chase.
39. **Sizing Unpaid Claims:** The chart on the next page shows Chase's own internal estimates of the number of reimbursement claims, declined as of late 2024, which



NAPIER NETWORK

could have been approved via call recordings or Voice Bio mismatch. Please note that while Chase does not generally pay Scam claims, in the chart below, the term "Scam" refers to Scam + Fraud combinations, described in detail elsewhere in the disclosure, in which Chase blocks the initial Scam transaction but the transaction is ultimately "authenticated" by the bad actor exploiting call center weaknesses.

40. All together, Chase internal estimates indicated that failure to Voice Bio and call recording data for reimbursement claim investigations had resulted in **\$42 million of claims denied in the past year**. Chase treats each of these categories as non-duplicative and non-overlapping:

- a. \$9.9 million Fraud claims based on Voice Bio
- b. \$9.0 million Scam + Fraud claims based on Voice Bio
- c. \$12.4 million Fraud claims based on call recordings
- d. \$10.7 million Scam + Fraud claims based on call recordings