UNITED STATES DISTRIC COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

THE PEOPLE OF THE STATE OF NEW YORK, by LETITIA JAMES, Attorney General of the State of New York, Plaintiff, v. CITIBANK N.A., Defendant.	Case No. 24 Civ. 0659

COMPLAINT

Plaintiff the People of the State of New York, by Letitia James, the Attorney General of the State of New York, bring this action against Citibank, N.A. ("Citi") and alleges as follows:

INTRODUCTION

1. The rapid growth of online and mobile banking in recent years has placed consumers in the crosshairs of increasingly sophisticated scams. Convincing impersonation scams by text message and over the phone, known as phishing, and mobile device hacks, such as SIM swaps, pose ever-present threats. Through these frauds, scammers gain access to consumers' hard-earned wages, savings, retirement nest eggs, and college funds. Scammers can then use online or mobile banking access to make purchases, transfer money through payment apps such as Zelle or Venmo or by wire transfer, and engage in other unauthorized payment activity.

2. Because scammers execute these frauds and unauthorized payments by electronic means, a landmark consumer protection law known as the Electronic Fund Transfer Act ("EFTA") provides substantial protection. As with credit cards, so long as consumers promptly alert banks

to unauthorized activity, the EFTA limits losses and requires reimbursement of stolen funds. These consumer protections cannot be waived or modified by contract.

3. Banks, as the sophisticated financial institutions that market and offer online and mobile banking directly to consumers, thereby are incentivized by the EFTA to deploy safety measures, security protocols, and other guardrails to prevent scammers from infiltrating online and mobile banking and engaging in unauthorized activity to steal consumer funds.

4. Or so it should be. As alleged herein, however, Defendant Citi has not deployed sufficiently robust data security measures to protect consumer financial accounts, respond appropriately to red flags, or limit theft by scam. Instead, Citi has overpromised and underdelivered on security, reacted ineffectively to fraud alerts, misled consumers, and summarily denied their claims. Citi's illegal and deceptive practices have cost New Yorkers millions.

5. Citi makes online and mobile banking available to consumers, which consumers can access using usernames and passwords, codes, or other security protocols, and through which consumers can review account information, deposit checks, and make electronic payments. In recent years, Citi has connected wire transfer services to consumers' online and mobile banking, providing consumers with direct electronic access to the wire transfer networks.

6. When scammers infiltrate consumers' online or mobile banking to initiate fraudulent wire transfers using this access, two things occur. *First*, scammers electronically instruct Citi to send tens of thousands of dollars or more by wire to third-party banks where scammers have set up dummy accounts. *Second*, scammers electronically instruct Citi to reimburse itself by debiting consumers' bank accounts. These electronic instructions, however, do not come from the actual consumers who are Citi account holders. Under the EFTA, Citi's electronic debits of consumers' accounts are unauthorized and Citi must reimburse all debited amounts.

7. Yet when panicked consumers notify Citi of fraudulent activity on their accounts, there is no mention of the EFTA. Nor did Citi take immediate action in the past to recover amounts it wired out. Instead, Defendant's representatives frequently assure consumers (falsely) that their money and accounts are secure and then instruct consumers to visit their local branches.

8. When consumers arrive at local branches, Defendant's representatives likewise say nothing about the EFTA. They instruct consumers to complete form "Affidavits of Unauthorized Online Wire Transfers," often telling consumers that Citi will not take any action to investigate their fraud claims until the affidavits are executed and notarized. Defendant's representatives also encourage consumers to include details on how they were scammed in those affidavits.

9. Unsuspecting consumers complete these affidavits believing they are necessary for Citi to investigate claims and reclaim their stolen funds. In fact, under cover of these coerced affidavits, Citi treats consumers' claims as subject to narrow commercial laws governing wire transfers rather than the EFTA's robust protections for unauthorized electronic payments. Citi then summarily rejects claims for reimbursement and instead blames consumers, relying on the same information that Defendant's representatives encourage consumers to share with Citi.

10. Citi relies on the Uniform Commercial Code ("UCC"). Under the UCC, banks are not required to reimburse payments for unauthorized wire transfers if they execute wire transfer requests in good faith and subject such requests to commercially reasonable security procedures that are to be negotiated between banks and their sophisticated commercial customers.

11. But consumers negotiate no security procedures with Citi. When consumers sign up for online or mobile banking they must agree to Defendant's online terms and conditions, under which Citi provides consumers with the means to electronically access their accounts. And while Citi promises its online and mobile banking will be safe and secure, the terms and conditions set

out weak security procedures, such as single-factor protocols relying on usernames and passwords, that are readily susceptible to breach by scams such as phishing or SIM swaps.

12. Citi's data security policies and procedures, its efforts to monitor, secure against, and defeat fraudulent activity in real time, and its responses to obvious red flags of identity theft and account takeover are haphazard and ineffective. Among other things:

a. Citi permits scammers to alter contact information, usernames, and passwords, upgrade accounts to access online wire transfer services, and consolidate funds across multiple accounts, all without subjecting to robust scrutiny scammers' subsequent requests to initiate large-dollar wire transfers that will empty consumers' accounts;

b. Citi fails to employ tools that effectively monitor and respond to anomalous consumer or account activity, such as wire transfers that are the first ever involving consumers' accounts, that are for out-of-the-ordinary amounts based on past activity, or that will effectively empty consumers' accounts; and

c. even when alerted to fraudulent activity, Citi does not effectively secure consumers' bank accounts, which remain vulnerable to scammers.

13. The results are devastating. Consumers lose tens of thousands of dollars or more by doing nothing more than clicking on a link in a text that appears to be from a trusted source, providing information on a call with a purported representative of Citi, or answering security questions on a website that looks official. These small acts, done in good faith by consumers who believe they are acting to secure their accounts or prevent fraud, result in large losses in minutes. Depression, shame, embarrassment, extreme stress, and financial strain often follow.

14. Plaintiff alleges that Defendant has violated New York Executive Law § 63(12) by engaging in repeated and persistent illegal conduct by:

a. failing to comply with the EFTA or the UCC in its handling of consumers' notices of fraudulent electronic payment activity (Counts I & IV);

b. failing to apply the EFTA to unauthorized electronic transfers that consolidate funds from multiple accounts into a single account (Count II);

c. employing adhesive online terms and conditions for consumer banking that violate the EFTA's anti-waiver provisions and the EFTA's requirement that contractual terms be clear and readily understandable (Count III);

d. failing to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of consumers' financial account information as required by New York's SHIELD Act (Count V); and

e. failing to maintain a data security program that is appropriately designed to detect, prevent, and mitigate identify theft in response to red flags indicative of possible identity theft, as required by applicable regulations (Count VI).

15. Plaintiff further alleges that Defendant has violated Executive Law § 63(12) and New York General Business Law § 349 by repeatedly and deceptively inducing consumers to enter into agreements setting forth inadequate security procedures, misleading consumers about their rights, depriving consumers of statutory safeguards, falsely promising consumers that their money is secure when it is not, tricking consumers into executing unnecessary affidavits, inflating the likelihood of recovery of stolen funds, and blaming the victims (Counts VII & VIII).

16. The Court should enjoin Defendant from engaging in illegal and deceptive conduct, should order Defendant to hire an independent third party to review its handling of consumers' claims of unauthorized payment activity in connection with fraudulent wire transfers, and should award restitution, disgorgement, damages, penalties, and other relief as appropriate.

PARTIES & JURISDICTION

17. Plaintiff is the People of the State of New York, by their attorney, Letitia James, the New York Attorney General ("OAG") and is authorized to take action to enjoin repeated and persistent fraudulent and illegal conduct under New York Executive Law § 63(12) and deceptive business practices under New York General Business Law ("GBL") § 349.

18. Defendant Citibank, N.A. is a national bank whose principal offerings include investment banking, commercial banking, cash management, trade finance, and e-commerce; private banking products and services; consumer finance, credit cards, and mortgage lending; and retail banking products and services. As of 2022, Citi held more than $1 trillion in deposits, including more than $400 billion in consumer deposits. Defendant is headquartered at 5800 South Corporate Place, Sioux Falls, South Dakota 57108. Defendant is the wholly owned subsidiary of Citigroup, Inc., headquartered at 388 Greenwich Street, New York, New York 10013.

19. Plaintiff has provided Defendant with notice as specified in GBL § 349.

20. This Court has subject-matter jurisdiction over this action because it presents a federal question, 28 U.S.C. § 1331, and because the state-law claims form part of the same case or controversy with those claims that present a federal question, 28 U.S.C. § 1367(a).

21. This Court has personal jurisdiction over Defendant because the causes of action arise from Defendant's contracting with New York residents to supply goods and services in New York and from Defendant's committing of tortious acts within and without New York causing injury to persons or property within New York. Fed. R. Civ. P. 4; CPLR 302.

22. Venue is proper in this district because Plaintiff resides in this district, a substantial amount of the transactions, practices, and courses of conduct at issue occurred within this district, and because Defendant conducts business in this district. 28 U.S.C. § 1391(b)(2).

FACTUAL ALLEGATIONS

I. CONSUMERS TODAY INCREASINGLY FACE HIGHLY SOPHISTICATED SCAMS SEEKING TO INFILTRATE ONLINE AND MOBILE BANKING

23. In 1978, consumer access to wire transfer networks was extremely limited—and continued to be for decades. A 2002 Congressional Research Service report on electronic payment systems in the United States, for example, did not even acknowledge the possibility of consumer use of the wire networks, defining the "primary wire transfer system" as a network that "transfers, disburses, and collects funds for depository financial institutions, corporations, and governmental agencies." And in its tri-annual studies of non-cash payment activity and trends in the United States, the Federal Reserve, as late as 2010, defined consumer or retail payments—as opposed to business or financial institution payments—to exclude wire transfers entirely.

24. The past decade, however, has seen a rapid expansion of widely available internet access, high-speed Wi-Fi, and mobile devices. With this changing environment came the rise of online and mobile banking, through which consumers became accustomed to accessing their bank accounts electronically, reviewing account balances and status online, going paperless, paying bills automatically, and engaging in a wide array of online and mobile banking activity.

25. These trends were further accelerated during the Covid-19 pandemic: one recent report stated that 87% of U.S. adults primarily bank online or on mobile devices.

26. With these shifts, banks began to market and provide electronic payment options directly to consumers, including the ability to seamlessly transfer money among bank accounts online or using mobile devices. Many banks also redesigned their payment systems to provide consumers with electronic access to wire transfer services over the internet or on mobile devices. Citi, for example, advertises to consumers the ability to "conveniently send money" same day by wire transfer and offers to waive wire transfer fees for certain account holders.

27. The result has been an enormous increase in consumer wire activity. According to the Federal Reserve, from 2012 to 2018, consumers' use of wire networks grew at double-digit percentage rates. And while wire transfer volume measured in dollars fell by 2.5% overall from 2015 to 2018, consumer wire transfer volume increased by 20% over the same period.

28. By 2018, consumer wire transfers amounted to more than $4.3 trillion annually, and consumer wire transfers constituted 11% of all wire transfers by transaction.

29. The explosion of online and mobile banking, including the ability to electronically access wire transfer services, has been accompanied by an explosion in frauds through which scammers attempt to infiltrate online or mobile banking to steal consumers' money.

30. One commonly used scam is an impersonation scam, also referred to as "phishing," through which scammers call or send emails or text messages to consumers pretending to be banks or other reputable institutions, such as the government or a well-known business. The purpose of impersonation scams is to trick consumers into providing personal or security information that can be used to fraudulently infiltrate consumer accounts, including online or mobile banking.

31. Phishing scams have grown rapidly over the last several years. In 2021, the FBI reported that these sorts of scams had grown by more than 1,000% from 2017 to 2021. The FTC similarly reported that impersonation scams are a leading source of fraud, amounting to more than 750,000 complaints and losses of more than one billion dollars in 2021 alone.

32. Another commonly used scam targets mobile device subscriber identity modules, or SIMs, that contain unique identifiers for consumers' mobile phones. These "SIM swaps" are done by obtaining personal identifying information via text message or the dark web, after which scammers contact mobile providers to activate new phones with consumers' stolen SIMs and

deactivate consumers' actual phones. Once in control, scammers can reset key apps on devices using text message authentication, including mobile banking and email apps.

33. The goal of these and other similarly sophisticated scams aimed at modern consumers is the same: gaining information sufficient to fraudulently infiltrate online and mobile banking. Scammers then are able to steal consumers' money through various means made available by consumers' banks, including online purchases using virtual debit cards, peer-to-peer payments such as Zelle or Venmo, purchases of gift cards or cryptocurrency, and wire transfers where banks have provided direct electronic access to the wire transfer networks.

34. The FTC reported that in 2022 alone, scammers stole hundreds of millions of dollars from consumers using text messages impersonating banks, delivery services, Amazon, and other common service providers. That same report indicated that the single most frequent party that scammers impersonated over text was consumers' banks.

35. These trends have affected Citi. For example, the number of complaints related to Defendant's handling of claims for fraudulent wire transfers submitted by consumers to the federal Consumer Financial Protection Bureau nearly tripled from 2020 to 2022.

36. And Citi is aware of the increased risks posed by scammers. Defendant's own ads state that "scammers are targeting payment methods that allow them to receive funds very quickly and which are difficult to recover," that "bad players are after your personal information because it's the key to your accounts," and that "phone takeover can put your money at risk."

II. THE ELECTRONIC FUND TRANSFER ACT: LANDMARK CONSUMER PROTECTION LEGISLATION GOVERNING ELECTRONIC PAYMENTS

37. Congress enacted the federal Electronic Fund Transfer Act in 1978, decades before banks provided direct electronic access to wire transfer networks via online or mobile banking, to clarify the rights and liabilities of consumers, banks, and other intermediaries for electronic

transfers of money. The EFTA and its implementing Regulation E ("Reg. E") are landmark protections that shift liability for unauthorized transfers from consumers to banks.

38. The EFTA governs any "electronic fund transfer," referred to herein as an "EFT," which it defines as any transfer of funds that is initiated through an electronic terminal, telephonic instrument, or computer that orders, instructs, or authorizes a financial institution, such as Citi, to debit or credit an account. 15 U.S.C. § 1693a(7). Everyday examples of EFTs include purchases made using debit cards, ATM withdrawals, direct deposits, online bill payments, peer-to-peer payments using mobile apps, transfers among consumers' accounts, and all other debits or credits initiated by computer or mobile device. *Id*; 12 C.F.R. § 1005.3(b)(1).

39. The EFTA and Reg. E protect consumers from unauthorized EFTs and other errors. EFTs are unauthorized when they do not benefit consumers and are made by persons who are not the consumers or other authorized users. 15 U.S.C. § 1693a(12). When scammers fraudulently infiltrate online or mobile banking to electronically execute transactions that cause banks, such as Citi, to move money into or out of consumers' accounts, these are unauthorized EFTs.

40. The EFTA's consumer protections for unauthorized EFTs adhere to a three-tiered structure that is based on when consumers provide notice of unauthorized EFTs to their banks:

a. *First*, when consumers notify banks of unauthorized EFTs within two business days of discovering the EFTs, their losses are capped at $50 or less, and banks must reimburse anything above $50. 15 U.S.C. § 1693g(a).

b. *Second*, when consumers notify banks of unauthorized EFTs within sixty days of discovering the EFTs, their losses are capped at $500, but only if banks prove that those losses would not have occurred had consumers reported the unauthorized EFTs within two business days rather than sixty. 15 U.S.C. § 1693g(a).

c. *Third*, when consumers do not notify banks of unauthorized EFTs within 60 days of discovery the EFTs, their losses are not capped, but only if banks prove that those losses would not have occurred had consumers reported the unauthorized EFTs within sixty business days rather than later. 15 U.S.C. § 1693g(a).

41. The EFTA and Reg. E also require banks to disclose the terms and conditions that apply to EFTs in readily understandable language. 15 U.S.C. § 1693c(a); 12 C.F.R. § 1005.4.

42. Consumer protections in the EFTA and Reg. E, including for unauthorized EFTs, cannot be waived or limited by any agreement, including consumers' deposit agreements, online account agreements, or fund transfer agreements with their banks. 15 U.S.C. § 1693l.

43. The practical result of the EFTA and Reg. E is that banks bear the bulk of losses when consumers' funds are lost due to scammers' large-dollar, unauthorized EFTs. Banks thus are incentivized to prevent unauthorized access to consumers' bank accounts through online or mobile channels, thereby fostering consumer confidence in the electronic banking system.

III. SCAMMERS' USE OF CONSUMERS' ONLINE OR MOBILE BANKING TO EXECUTE WIRE TRANSFERS RESULTS IN UNAUTHORIZED EFTS BY CITI

44. Wire transfers are electronic means of moving money between banks over a secure network. The first wire network was developed by the Federal Reserve as a faster and more secure way to settle amounts owed between banks located in different geographic areas, replacing the need for banks to settle accounts through physical delivery of cash or gold.

45. Over time, the wire networks grew commercially as alternatives for businesses to sending paper instruments such as checks or transporting cash or gold to settle accounts. These transactions were historically done in person, over the phone, or by other means agreed upon between the businesses that accessed the wire transfer networks and their banks.

46. The simplest and most common form of a wire transfer involves four parties: the sender, who wants to send money; the beneficiary, to whom the sender wants to send money; the receiving bank, a bank that receives an instruction to execute a wire transfer (and where the sender often has a bank account); and the beneficiary bank, a bank at which the beneficiary has a bank account. The actual movement of money from the sender to the beneficiary involves several fund transfers, only some of which actually involve the wire transfer networks.

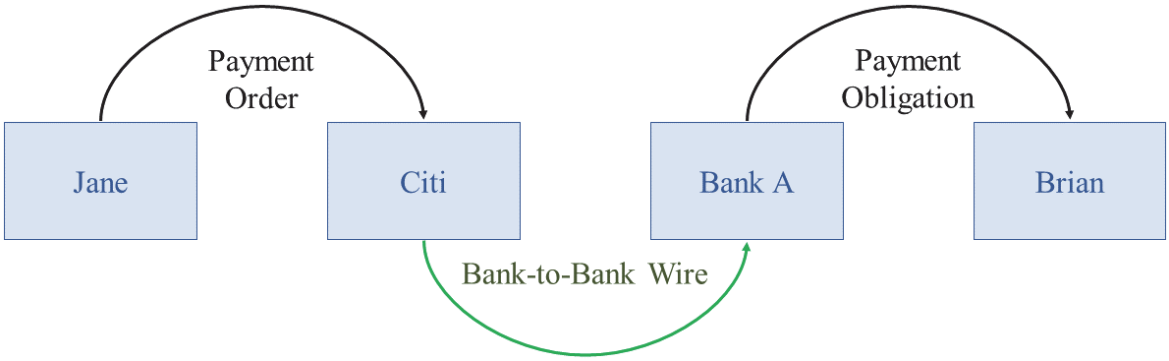
47. The first step is a "Payment Order," which is an instruction sent by the sender to the receiving bank instructing it to pay or cause another bank to pay the beneficiary. U.C.C. § 4-A-103(1)(a). Payment Orders can be sent orally, such as by visiting a local branch to request a wire transfer, electronically, such as online or using a mobile device, or in writing.

48. For example, if Jane, who has a bank account at Citi, wants to send $1,000,000 by wire to Brian, who has a bank account at Bank A, Jane will send a Payment Order to Citi instructing Citi to cause Bank A to pay $1,000,000 into Brian's bank account. Jane is the sender, Citi is the receiving bank, Brian is the beneficiary, and Bank A is the beneficiary bank.

49. When a receiving bank accepts a sender's Payment Order, it sends a new Payment Order, either directly to the beneficiary bank if both banks participate in a common wire network, or through one or more intermediary banks, in which case each bank accepts the prior Payment Order and issues a new Payment Order until the final Payment Order is accepted by the beneficiary bank. The simplest form—transmission of a Payment Order directly from the receiving bank to the beneficiary bank over a wire network—is referred to herein as a "Bank-to-Bank Wire."

50. When a beneficiary bank accepts the final Payment Order, it becomes obligated to pay the amount in question to the beneficiary. U.C.C. § 4-A-404(1). In the example, the chain of

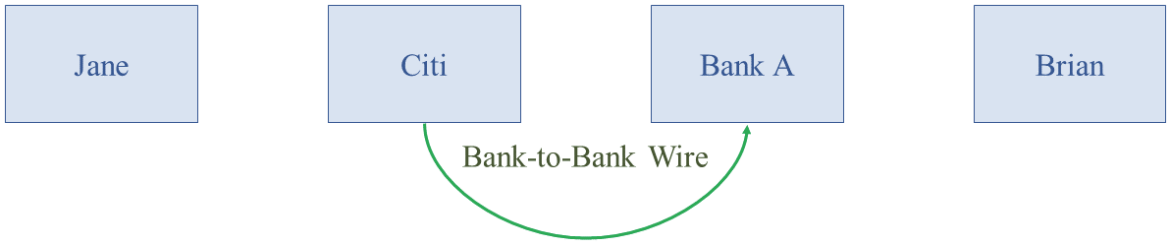
events for Jane to send $1,000,000 by wire to Brian consists of a Payment Order from Jane to Citi, a Bank-to-Bank Wire from Citi to Bank A, and a payment obligation from Bank A to Brian:



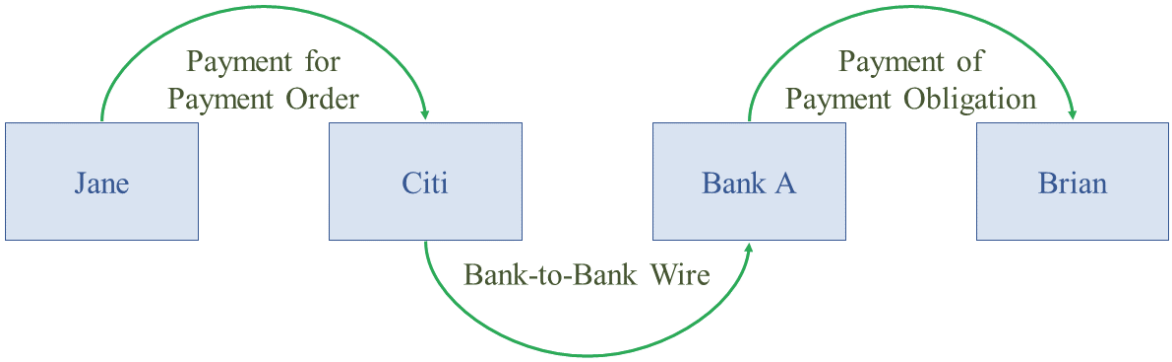
51. Bank-to-Bank Wires are fast and efficient because the participating banks agree to a predetermined set of rules and processes for settlement, netting out obligations across millions of dollars of transfers every day. For example, banks that participate in Fedwire, one of the two primary domestic wire networks, have master accounts with the Federal Reserve. When a receiving bank sends a Payment Order through Fedwire, a Federal Reserve bank will debit the receiving bank's master account and credit the beneficiary bank's master account. Similarly, for banks that participate in the Clearing House Interbank Payments System, or CHIPS, settlement occurs at the end of the day, when CHIPS nets all incoming and outgoing Bank-to-Bank Wires for each bank. Those banks whose outgoing payments exceeded their incoming receipts then immediately send, via Fedwire, funds to cover the shortfall to a CHIPS settlement account. CHIPS then sends those funds to the banks whose incoming receipts exceeded their outgoing payments.

52. As a result of these agreements among the banks who are direct participants in the wire transfer networks, when a beneficiary bank receives a Payment Order from a receiving bank over a wire network, the beneficiary bank need not analyze receiving bank's creditworthiness or assess the likelihood that the receiving bank will pay. The beneficiary bank can simply accept the Payment Order. Today, acceptance of interbank Payment Orders is near instantaneous.

53. A Bank-to-Bank Wire, however, is a movement of money between banks. While initiated by a sender's Payment Order to the receiving bank and resulting in the beneficiary bank's payment obligation to the beneficiary, money in a Bank-to-Bank Wire moves only from a receiving bank to a beneficiary bank (at times through intermediary banks). In the example, no money moves, either from Jane to Citi, or from Bank A to Brian, in the Bank-to-Bank Wire:



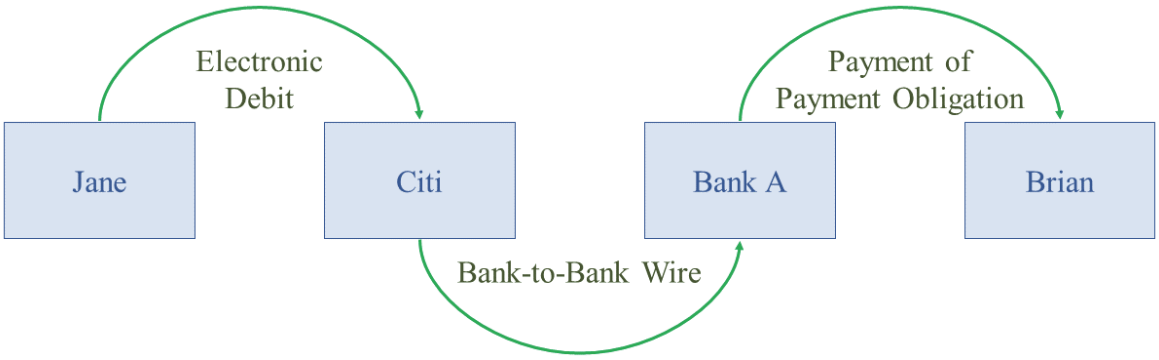
54. Other fund transfers occur in relation to a Bank-to-Bank Wire, but the transfers generally do not take place over the wire networks. In connection with a Bank-to-Bank Wire, the sender is obligated to pay for the initial Payment Order, U.C.C. § 4-A-402(2), while the beneficiary bank, upon accepting the final Payment Order, is obligated to pay the beneficiary, *id*. § 4-A-404(1). In the example, Jane is obligated to pay $1,000,000 to Citi for accepting her initial Payment Order and Bank A is obligated to pay $1,000,000 to Brian when it accepts Citi's Payment Order. But the payments made to satisfy these obligations are independent of the Bank-to-Bank Wire:



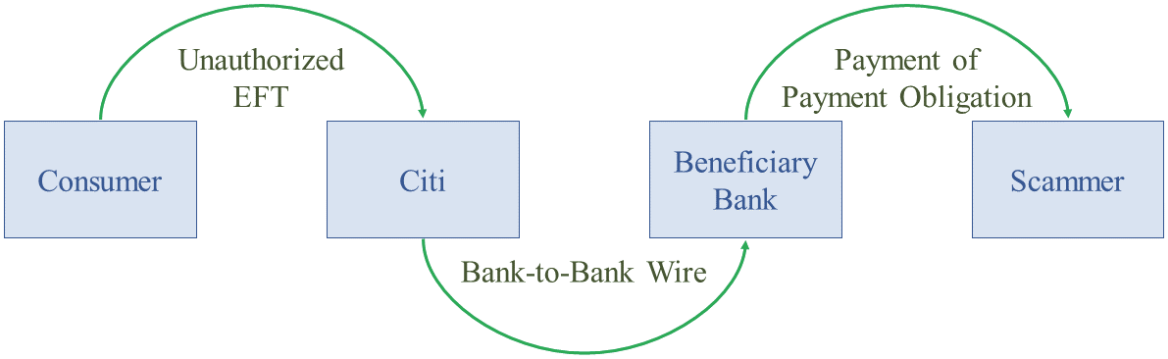
55. A sender can pay for a Payment Order in many ways. A sender who submits a Payment Order in-person at a local branch might pay in cash, write a check, or verbally authorize

the bank to debit a bank account. A sender who submits a Payment Order in writing might include a check, credit card authorization, or debit authorization with that writing. And a sender who submits a Payment Order electronically might send a credit card or debit authorization.

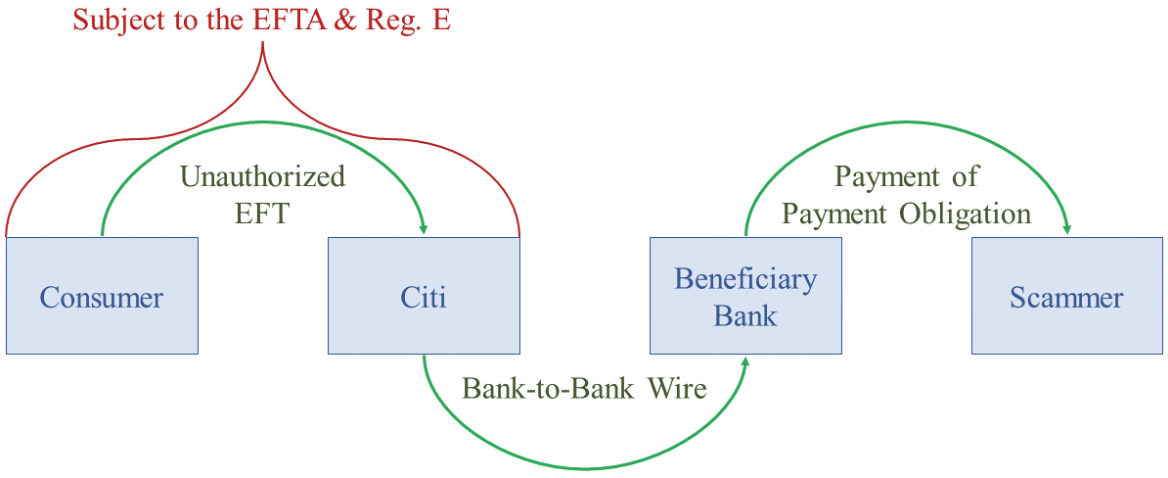
56. When Citi receives Payment Orders from consumers initiated electronically via online or mobile banking, Citi applies its Agreement for Online Funds Transfers or comparable agreements. These agreements provide that consumers' electronic transfer requests to Citi, such as Payment Orders, also act as electronic authorizations for Citi to debit consumers' bank accounts to pay for the transfers. In the example, when Jane uses online or mobile banking to send her Payment Order to Citi, she also electronically authorizes Citi to debit her bank account:



57. But when Citi receives Payment Orders from scammers initiated electronically after infiltrating consumers' online or mobile banking, it is the scammers, and not the consumers, who purport to electronically authorize Citi to debit consumers' bank accounts. These electronic debit authorizations do not come from the affected consumers and the resulting debits do not benefit those consumers. Citi's electronic debits therefore are unauthorized EFTs. In the example, if Brian is not a known party but is instead a scammer who fraudulently infiltrates a consumer's online or mobile banking to electronically send a Payment Order and related debit authorization to Citi, the resulting debit by Citi of the affected consumer's account is an unauthorized EFT:



58. Given the lightning-fast speed at which wire networks operate, scammers' executions of these frauds are nearly instantaneous: tens of thousands of dollars disappear from consumers' bank accounts and in an instant reappear in accounts at beneficiary banks for scammers to steal. And as detailed below, Citi characterizes this complex set of transfers as a single, instantaneous "wire transfer" to confuse, mislead, and deprive affected consumers of their legal rights. But the payment mechanics are clear: each of (i) the unauthorized EFTs that Citi executes to pay itself for the fraudulent Payment Orders, (ii) the Bank-to-Bank Wires between Citi and the beneficiary banks, and (iii) the beneficiary banks' payments into scammers' accounts are independent fund transfers. And each is subject to particular laws, including—with respect to at least the unauthorized EFT from a consumer's account to Citi—the EFTA and Reg. E:



IV. CITI ILLEGALLY ATTEMPTS TO END-RUN THE EFTA AND REG. E BY DECEIVING CONSUMERS & DENYING CLAIMS AS A MATTER OF COURSE

59. When consumers learn that their online or mobile banking has been compromised and notify Citi of stolen funds in connection with scammers' fraudulent Payment Orders and Citi's unauthorized EFTs, Defendant's representatives will lock consumers' bank accounts and instruct consumers to visit their local branches. As a result, investigations are delayed hours or days, providing time for scammers to escape with stolen funds held at beneficiary banks.

60. When consumers visit their local branches, Defendant's representatives state that before Citi will investigate the fraudulent activity or take any other action, consumers must execute and have notarized a form "Affidavit of Unauthorized Online Wire Transfer." These affidavits make no reference to the EFTA, to Reg. E, or to Citi's unauthorized EFTs.

61. When completing these affidavits at local branches, Defendant's representatives often encourage consumers to include specific details regarding how scammers infiltrated their online or mobile banking, at times even filling out the affidavits for consumers. Citi often relies on this information when it later blames consumers and denies their claims.

62. Under the guise of these affidavits, Citi treats consumer claims as solely claims for unauthorized Payment Orders governed by the UCC. Citi does not apply the EFTA to its own unauthorized EFTs initiated electronically by scammers, citing a narrow but inapplicable exclusion for Bank-to-Bank Wires. Citi does not provisionally credit consumers' accounts. Citi does not cap consumers' liability for unauthorized EFTs. And Citi does not treat intra-bank transfers among accounts that provide funds for fraudulent activity as unauthorized EFTs.

63. Citi's investigations that follow submission of affidavits are ineffective, pro forma, and not reasonably tailored to mitigate the security failure that led to the unauthorized EFTs and

consumer losses. Indeed, Defendant's representatives responsible for conducting and completing investigations do not always even speak directly to complaining consumers.

64. These investigations conclude when Citi sends consumers form letters in the mail titled "Decision on Fraud Claim" that refer to an "Unauthorized Wire Claim" and make no mention of the EFTA, Reg. E, or Citi's unauthorized EFT. This typically occurs in 30 to 60 days and receipt of the letter can be the first time that consumers have heard anything from Citi.

65. Defendant's form letters make no reference to the EFTA or Reg. E. The form letters do not describe the scope of the investigation, what actions Citi took, or what evidence Citi relied upon. The form letters merely assert, in one or two sentences, one of a few predetermined grounds for denying claims. These predetermined descriptions of Citi's purported findings include:

- "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."
- "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam."
- "No new information was received or discovered that would change the denial decision."

Citi's form letters do not describe, cite, or append as exhibits any evidence for these predetermined conclusions. Indeed, Citi does not even update the boilerplate language in the first bullet above to reflect whether its investigation involved one or more fraudulent transactions.

66. Other than blaming consumers, Citi's form letters provide no details on the bases for its denials. The letters do not, for example, state what security procedures (discussed below) Citi employed, nor do they provide any evidence that those procedures were followed.

V. CITI APPLIES THE UCC AND NOT THE EFTA TO CONSUMERS' CLAIMS FOR FRAUDULENT WIRE TRANSFERS AND UNAUTHORIZED EFTS

67. Citi treats the Affidavit of Unauthorized Online Wire Transfers it receives solely as claims by consumers for reimbursement for unauthorized Payment Orders under the UCC.

68. Article 4-A of the UCC was adopted after the EFTA and was crafted to not interfere with the EFTA. In particular, Article 4-A expressly provides that it does not apply to transfers that are governed by the EFTA, U.C.C. § 4-A-108(1), and that in the event of any inconsistency between the UCC and the EFTA, the EFTA governs, *id*. § 4-A-108(3). Citi's discarding of the EFTA and Reg. E in favor of the UCC is not consistent with this legal framework.

69. Nor could Citi successfully rely on the UCC to shield itself from liability for these frauds in any event. The UCC generally provides that banks must reimburse customers for unauthorized Payment Orders. U.C.C. § 4-A-204(1). However, banks and their customers can agree upon specific security procedures for verifying Payment Orders that the banks receive. *Id*. § 4-A-201. And if banks can prove that these procedures are commercially reasonable, were followed, and that Payment Orders were accepted in good faith, the UCC provides that the banks need not reimburse customers, even for unauthorized Payment Orders. *Id*. § 4-A-203.

70. Whether particular security procedures are commercially reasonable is determined by a variety of factors, including the circumstances of the customer known to the bank, such as the size, type, and frequency of Payment Orders normally issued by the customer to the bank.

71. The UCC specifies that use of an authorized signature specimen alone is not a sufficient security procedure. Consistent with this approach, legal and policy consensus is that comparable single-factor procedures, such as an online username and password, also are not a commercially reasonable security procedures standing alone. For example, the Federal Financial Institutions Examination Council ("FFIEC"), a federal interagency body that prescribes uniform

procedures for U.S. financial institutions, has publicly cautioned that use of single-factor authentication is inadequate either to safeguard against scammers fraudulently infiltrating customers' online or mobile banking or to prevent widespread payment fraud.

72. Multi-Factor Authentication ("MFA"), as opposed to single-factor authentication, is one available control for financial institutions to prevent fraudulent online or mobile activity. MFA requires more than one distinct authentication factor. The factors are something consumers know (such as usernames and passwords), something consumers have (such as mobile devices), and something consumers are (such as fingerprints or other biometric identifiers).

73. MFA, however, has been shown to be ineffective when used alone. Consumers' email accounts, browsers, and mobile devices are common access points for scammers. Thus, the FFIEC recommends that financial institutions employ layered security approaches, which incorporates multiple preventative, detective, and corrective controls, and which is designed to compensate for potential weaknesses in any one control, including MFA.

74. A critical aspect of layered security is an evaluation of consumers and their account histories, including usage patterns, the frequency of high-dollar transactions, and whether transactions or other recent online behaviors are anomalous. Nacha, the entity formerly known as the National Automated Clearinghouse Association, which manages the ACH payment network, has commented that commercially reasonable, risk-based approaches to security will consider account characteristics and anomalous behavior. When banks identify anomalous behavior or transactions, commercially reasonable and effective controls will prompt the banks to employ more robust procedures to scrutinize and verify electronic payment activity.

75. In addition to MFA, layered security can include a number of other effective controls, such as requiring dual authorization through different access devices, such as a phone

call to a landline and a text message to a mobile device, limits on transaction frequency or size based on prior usage patterns, and the use of enhanced authentication techniques after changes to account types or characteristics, such as account upgrades or changes to passwords.

76. Another aspect of effective layered security is sufficient training and controls for call center and fraud prevention employees. Scammers use engineering and other sophisticated techniques to deceive these employees into resetting passwords or granting scammers access to accounts, including online or mobile banking. Commercially reasonable security procedures are those that employ monitoring and processes to defeat fraudulent transactions in real time.

VI. CITI PROMISES CONSUMERS SAFE AND SECURE ONLINE AND MOBILE BANKING BUT IN FACT EMPLOYS WEAK SECURITY PROCEDURES

77. When consumers open checking or savings accounts with Citi, they must agree to Citi's standard-form client manual for consumer bank accounts. These agreements are not subject to any negotiation. And critically, whatever terms these or other agreements contain, the contracts cannot waive, limit, or modify the core consumer protections provided by the EFTA.

78. Defendant's standard-form client manual for consumer bank accounts requires that Citi verify the authenticity of Payment Orders through direct, personal contact. It contains the following security procedures provision (emphasis added in bold and italics):

> When you place an order for a funds transfer, we will follow a security procedure established for your protection and ours to verify that the transfer has been properly authorized. You understand that the security procedure is designed only to verify the source of the funds transfer instruction and not to detect errors in the content of that instruction or to prevent duplicate transfers. The procedure depends on the means by which you provide instructions to us. ***Unless we agree on another security procedure, you agree that we may confirm the authenticity and content of instructions by placing a call to any authorized signer on your account***. By placing a transfer order, you agree to our use of the applicable security procedure. You agree to be bound by any funds transfer request that Citibank receives and verifies in accordance with the security procedure outlined above.

79. Citi makes a concerted effort to promote online and mobile banking. Its ads say that the bank is "excited to share" online and mobile banking experiences. Citi's website reads: "Online Banking with Citi Made Easy" and promises simple account management, hassle-free fund transfers, and convenient payments, among other features. Citi's website shows consumers how to review account information, deposit checks, and locate ATMs, all online.

80. Citi similarly pushes banking through its mobile app, promising to give consumers "the power of simplicity to manage all your finances, virtually anytime and anywhere!"

81. Citi's efforts to push consumers toward online and mobile banking is a conscious business decision by the bank to compete and drive revenue. Citi has publicly acknowledged that it is "clear that for us at Citi, mobile banking is a significant channel." As one of Citi's regional heads of digital banking states in an online advertisement for Citi's online banking experience, "mobile represents the best opportunity to extend the reach of our services."

82. Central to Citi's efforts to promote online and mobile banking are promises of safe and secure electronic banking experiences. Citi advertises its online banking platform as "an affordable account with a range of convenient Citi digital services," promising that security "is a priority for Citi with 24/7 fraud detection services and security features to keep your account information protected." And Citi represents that it is "constantly working to safeguard your account." It further promises consumers that Citi is "here to keep your card protected."

83. Among its online advertising, Citi represents the following to consumers:

- "As always at Citi, your security is important to us."
- "We, at Citi, consider your security to be the topmost priority."
- "At Citi, we take protecting your account seriously."

84. Despite these promises, when consumers enroll in online and mobile banking with Citi, they must agree to Defendant's adhesive online terms and conditions, which supplant the direct-contact security procedures in the client manual. These revised security procedures are not negotiated with consumers and rely primarily on single-factor authentication—consumers' usernames and passwords—while removing any requirement of direct, personal contact. And many of the potential security procedures that would typically be expected are made entirely discretionary depending on Citi's whims. In particular (emphasis added in bold and italics):

> ***Citi Online has been designed to reduce the possibility of fraud and error by placing the issuance of a User ID and Passwords ("Codes")*** under your control so that accounts may be accessed only upon entry of valid Codes. ***You authorize Citibank to treat any instruction made on Citi Online with valid Codes as if the instructions had been made in writing and signed by you.*** Unless there is substantial evidence to the contrary, Citibank records will be conclusive regarding any access to, or action taken through, Citi Online. You are responsible for maintaining the confidentiality of the Codes and you will not allow any person (including another Citibank customer or your employee) to use the Codes. You agree to inform Citibank promptly of any discrepancies that you discover. ***Citibank will therefore consider any access to Citi Online through use of valid Codes to be duly authorized, and Citibank will carry out any instruction given regardless of the identity of the individual who is actually accessing the system***. You confirm the security system and controls are commercially reasonable and appropriate for you. When you place an order for a funds transfer (including a wire or cable transfer), ***Citibank may follow a security procedure*** established for your protection that ***may entail*** a telephone call or other required contact with you or from you prior to acting upon your instructions. In certain instances, Citibank may also decline to act upon your instructions. Citibank ***may employ other controls*** to verify your identity as a condition of granting access including the collection and use of data that authenticate you or your computer. You agree to these security procedures, and acknowledge that if contacted, either by telephone or electronically, you will act or respond in compliance with requests resulting from these security procedures and will be bound by any resulting transfer or decision not to act upon your instructions or to deny access to persons purporting to be you.

85. The above security procedures in Citi's online terms and conditions appear in the 21st paragraph of dense, legalistic text. And depending on how consumers enroll in online or mobile banking with Citi, they need not scroll past these terms or even open them at all.

86. Nor does Citi encourage consumers to closely review these security procedures. One Citi advertisement that walks through the steps to sign up for electronic banking, for example, shows a consumer scrolling through just a few paragraphs of disclosures while not opening the online account agreement at all—the only place the revised security procedures would appear—before scrolling back up to e-sign the agreement. Another Citi online advertisement shows a consumer registering for Citi's mobile app by opening the lengthy terms and conditions and then clicking "done" before even scrolling to the second paragraph, let alone the twenty-first.

87. Citi's security procedures also do not clearly disclose that Citi is no longer required to make direct, personal contact to verify that Payment Orders are in fact authorized by account holders, even in the presence of red flags. Nor is there any opportunity provided by Citi during the sign-up process for consumers to negotiate alternative procedures, such as the dual authorization protocols or physical tokens that Citi makes available to its commercial customers.

88. Defendant's procedures also contain superficial references to telephone calls, text messages or other controls—the sorts of checks that consumers are used to for anomalous activity on credit cards and other transactions—thereby suggesting that Citi will take similar steps to prevent fraudulent online or mobile banking activity. The procedures do not, however, make clear either that these procedures are discretionary or that by signing up for online or mobile banking consumers have agreed to security procedures that purport to bind them to any actions taken by anyone—even scammers—who have access to consumers' usernames and passwords.

89. Finally, Citi's online terms and conditions purport to alter the legal framework for EFTs in violation of the EFTA's anti-waiver provisions. For example, the terms and conditions provide that Citi may treat EFTs made using consumers' username and password as "authorized" while the EFTA requires persons to have actual authority for authorized EFTs—not just usernames

and passwords. The terms and conditions also alter the burden of proof and Citi's obligations to undertake a reasonable investigation under the EFTA and Reg. E, instead providing that Citi may deem its records "conclusive" in the absence of "substantial" contrary evidence.

VII. CITI'S SECURITY PROCEDURES ARE DISORGANIZED, HAPHAZARD, AND INCAPABLE OF EFFECTIVELY SAFEGUARDING CONSUMER FUNDS

90. While Citi is aware that scammers pose an increasing threat to consumers, the weakened security procedures set out in its electronic banking agreements are utterly ineffective at preventing consumers from falling victim to scams and losing significant sums.

91. When scammers fraudulently infiltrate consumers' online or mobile banking with Citi, the process to execute a Bank-to-Bank Wire online is quick and easy.

92. *First*, scammers must ensure that consumers' online or mobile banking accounts have been linked to the wire transfer networks. If the infiltrated accounts are not linked, scammers can either upgrade account types to those that are linked to the wire networks or can enroll directly in electronic wire transfer services—all of which can be done in moments.

93. *Second*, scammers must create new payees, who are the parties (typically scammers or their co-conspirators) that will act as the beneficiaries in the fraudulent Bank-to-Bank Wires that follow. To do so, scammers enter information (without authorization) into Citi's online or mobile banking platform about the payees, including names and account information.

94. *Third*, scammers must determine the amount of funds available. Where consumers have multiple Citi accounts, such as multiple checking or savings accounts, scammers frequently consolidate funds into one account by making intra-bank transfers, leaving the other accounts with near-zero balances. This avoids any additional scrutiny that might attend the rapid sending of multiple Payment Orders. These intra-bank transfers are done electronically and without triggering any heightened scrutiny, security procedures, or notice to consumers.

95. *Fourth*, scammers must use consumers' online or mobile banking to both send electronic Payment Orders instructing Citi to execute Bank-to-Bank Wires and to electronically authorize Citi—without consumers' knowledge or consent—to debit consumers' accounts.

96. *Fifth*, consistent with the online terms and conditions, Citi may perform whatever security procedures it determines to apply, in its sole discretion. This might include requests for verification via text message to mobile phone numbers that scammers have already SIM swapped, requests for email verification sent to email accounts that scammers have fraudulently infiltrated, or one-time codes sent to the mobile phones of consumers who have been deceived into sharing those codes with scammers pretending to be Citi representatives over the phone.

97. *Sixth*, if Citi accepts scammers' fraudulent Payment Orders, Citi will send new Payment Orders over wire networks to beneficiary banks. Money will then be moved between Citi and the beneficiary bank in the manner predetermined by the wire network. Internal Citi records of these Bank-to-Bank Wires identify Citi's own accounts (not consumers' accounts) as the sources of the funds and the beneficiary bank's own accounts as the recipients.

98. *Seventh*, per its account agreements, Citi will treat scammers' fraudulent Payment Orders as electronic authorizations to debit consumers' accounts to repay itself for the Payment Order, plus fees. Citi will execute unauthorized EFTs from consumers' accounts.

99. The amount of time between when scammers first fraudulently infiltrate online or mobile banking and when funds are stolen can be mere minutes. As a result, scammers' entire fraud can be executed hours, if not days, before consumers discover missing funds.

100. As scammers execute steps one through six above, Citi regularly fails to account for obvious red flags, employs inconsistent approaches to verification, does not react quickly to real-time notices of fraudulent activity, and needlessly delays efforts to recover stolen funds.

A. Citi's Security Procedures Fail to Defeat Fraudulent Payment Orders in the Face of Anomalous Account Activity and Other Clear Red Flags

101. For example, scammers, after fraudulent infiltrating consumers' online or mobile banking, can change passwords for account access. This locks consumers out and ensures that if they notice fraudulent activity in real time they cannot access online or mobile banking to attempt to stop that fraudulent activity. Yet when Citi receives Payment Orders tied to accounts whose passwords were altered hours or even minutes earlier, Citi does not always apply its most robust verification procedures to safeguard against potentially fraudulent Payment Orders. Nor does Citi respond by treating the transaction as an indication of possible identity theft.

102. Citi similarly does not employ its most robust security procedures in the face of other indicators of fraudulent activity, such as Payment Orders involving accounts whose status were recently upgraded, accounts that were recently enrolled in online wire transfer services, or accounts where the username or contact information was recently altered. The presence of these anomalous activities does not automatically trigger the most robust verification procedures that Citi employs or cause Citi to review the accounts in question for possible identity theft.

103. Citi likewise fails to account for intra-bank transfer activity when evaluating new Payment Orders. When scammers use intra-bank transfers to empty accounts and consolidate funds into a single bank account that is then used to send to Citi a large fraudulent Payment Order, Citi's internal procedures does not flag this account activity as suspicious in any way.

104. Citi also does not apply its most robust verification procedures to Payment Orders received within minutes of rejected Payment Orders involving the same accounts. At times Citi cancels fraudulent Payment Orders after it is unable to verify those orders directly—either because Citi is unable to contact consumers directly or because scammers provide inaccurate information when contacted. Yet when scammers submit new Payment Orders minutes later using the same

accounts for the same amounts, no heightened scrutiny is applied. To the contrary, at times Citi employs weaker verification procedures to the subsequent fraudulent Payment Orders.

105. Nor do Citi's security procedures meaningfully account for consumer or account characteristics. Consumers could be Citi account holders for decades, having never sent a Payment Order over years and years of account activity, and yet first-time Payment Orders purporting to be from such consumers do not trigger Citi's most robust verification procedures, nor do such red flags prompt Citi to evaluate whether the account has been subject to identity theft. This is true even when Payment Orders are received hours or minutes after other red flags, such as changes to passwords, preceding intra-bank account transfers, or upgraded account statuses.

106. Citi also does not subject Payment Orders that are anomalous based on consumers' historical account activity, such as Payment Orders for substantial amounts or that will result in near-zero account balances, to its most robust verification procedures as a matter of course.

B. Citi's Security Procedures Do Not Effectively Respond to Notices of Unauthorized Payment Orders or Defeat Ongoing Fraudulent Activity

107. Citi exacerbates its failure to design and implement effective front-end safeguards that identify and defeat fraudulent Payment Orders by employing ineffective processes for consumers who attempt to defeat fraudulent Payment Orders in real time.

108. One security procedure Citi may (in its sole discretion) employ is a simultaneous text message and email describing online activity and asking consumers to respond via text message or click a button in an email confirming or denying the legitimacy of a transaction. If consumers deny the legitimacy, Citi then instructs them to contact its fraud prevention department. But the initial text or email indications of fraud are not sufficient to secure consumers' accounts. While consumers are on (often lengthy) holds waiting for Defendant's representatives to come on

the line, scammers remain able to remove temporary holds and proceed with fraudulent Payment Orders electronically, thereby causing Citi to execute unauthorized EFTs.

109. Frightened and panicked consumers who are being contacted by Citi about fraudulent activity involving large sums, and who reasonably worry that the text messages or emails are themselves scams, at times decide to hang up and call a trusted number (such as the customer service line on their debit cards) or rush to their local branch. Citi itself encourages such precautions, warning consumers: "If you have any doubt, contact the company directly." But calls and visits take time, involving lengthy holds and transfers. Meanwhile, consumers' original responses via text or email that Payment Orders were not legitimate do not prevent scammers from removing holds and successfully sending Payment Orders electronically.

110. When consumers finally do reach Defendant's customer service line, moreover, poorly trained Citi representatives can do little to assist them. First-line representatives for Citi are not always empowered to directly lock accounts or reject Payment Orders. At best, they can transfer consumers to Citi's fraud prevention department, placing them back on hold.

111. Meanwhile, consumers' statements to Defendant's representatives that scammers are attempting to fraudulently send Payment Orders using consumers' bank accounts do not fully secure consumers' accounts. Scammers remain able to satisfy different security procedures working with Defendant's other representatives while consumers remain on hold, after which Citi will accept fraudulent Payment Orders and execute unauthorized EFTs.

112. Even reaching fraud prevention is not always enough. Scammers who have fraudulently obtained access to online or mobile banking can access all available bank accounts. But if consumers alert Citi fraud prevention about suspicious activity on a single account, Citi does not necessarily secure all accessible accounts. In such circumstances, scammers remain able to

execute fraudulent Payment Orders involving consumers' other, unsecured bank accounts during the period before consumers are able to physically visit their local branches.

113. And Citi's instructions that consumers must visit local branches to secure their accounts leaves consumers who are unable to immediately and quickly do so vulnerable and is not an appropriate response to notification of identity theft. Elderly consumers, consumers who may be recovering from medical procedures or are otherwise unable to immediately leave home, consumers who are living in areas where severe weather is ongoing, and consumers who live substantial distances from their closest branch are particularly at risk.

VIII. AFTER CONSUMER FUNDS ARE STOLEN, CITI DECEPTIVELY PROMISES CONSUMERS THAT SAFEGUARDS ARE IN PLACE TO PROTECT THEM

114. Once Citi executes unauthorized EFTs from consumers' accounts to repay itself for scammers' fraudulent Payment Orders, Defendant and its representatives deceive consumers through promises of account security and high prospects of prompt recovery.

115. Defendant's representatives, after instructing consumers to travel to their local branches to transfer funds to new accounts, assure consumers that their accounts have been secured and any fraudulent activity will be blocked. But scammers who retain access to consumers' online or mobile banking can and do defeat blocks and proceed with fraudulent Payment Orders.

116. Defendant's representatives also often reflexively assure consumers that because fraudulent activity caused consumers' losses, consumers will receive their money back.

117. But historically Citi has made no effort to immediately contact beneficiary banks in response to notices of fraudulent activity either to request that stolen funds be frozen or returned. Citi also has required that consumers explicitly request outreach to beneficiary banks before it will do so in real time. As a result, scammers are able to access and withdraw funds held at beneficiary banks even after consumers have provided notices of fraudulent activity to Citi.

118. Nor does Citi automatically initiate investigations or report fraudulent activity to police or law enforcement authorities when consumers first report that activity to Citi. Instead, Defendant's representatives instruct consumers to visit their local branches to report the activity and initiate investigations—which in turn requires consumers to complete, execute, and notarize the required affidavits. If consumers do not take these steps, Citi takes no further action.

119. Finally, even if Citi determines that consumers should be refunded funds stolen in connection with unauthorized Payment Orders initiated through online or mobile banking, Citi merely credits consumers' accounts; it does not always add statutorily required interest.

IX. CITI'S INEPT HANDLING OF POTENTIALLY FRAUDULENT ONLINE ACTIVITY CAUSES SUBSTANTIAL HARM TO NEW YORK CONSUMERS

120. Citi's refusal to adhere to the EFTA's investigation, provisional credit, and reimbursement requirements for the unauthorized EFTs it executes in connection with fraudulent Payment Orders, Defendant's lax security procedures and protocols to detect and defeat fraudulent Payment Orders, and Citi's ineffective monitoring, real-time response, and investigation of notices of fraudulent payment activity, have caused tremendous harm to New York consumers.

121. Scammers have diverted millions of dollars from New York consumers as a direct result of Citi's illegal and deceptive acts and practices. Consumers have lost their life savings, their children's college funds, or even the money needed to support their day-to-day lives.

122. The harm consumers suffer does not end with the lost money. Consumers who have lost substantial amounts due to scams and are unable to recover that money often feel a deep sense of shame or fear. They suffer from increased levels of stress, both from the loss itself and from the inability to understand what investigation is being done on their behalf. And consumers often are forced to turn to costly sources of funds to replace savings built up over decades.

123. Consumer A. Consumer A has been a Citi banking customer for decades. She recalls sending Citi one or two Payment Orders several years ago, before online banking.

124. On October 26, 2021, Consumer A received a text message that appeared to be from Citi. The message requested that Consumer A log onto a website to provide requested information or call her local branch. Consumer A clicked the link to the website, which appeared to be a website affiliated with Citi. Consumer A did not provide any information.

125. Concerned that the message might be a scam, Consumer A called her local branch. Defendant's representative, after Consumer A described the text message and website, responded "Don't worry about it, it happens all the time" and reminded Consumer A that Citi had security protocols in place. Defendant's representative did not place any hold on Consumer A's account, nor did he transfer Consumer A to Defendant's fraud prevention department.

126. Three days later, on October 29, 2021, Consumer A logged onto her email account and discovered that in the span of a few hours that day a scammer had changed her electronic banking password, enrolled her account in online wire transfer services, electronically attempted but failed a $39,999 wire transfer, and electronically executed a $40,000 wire transfer.

127. In particular, account records reflect that at 4:34 p.m. on October 29, 2021, a scammer electronically transferred $70,000 from Consumer A's savings account to her checking account. Consumer A did not make, authorize, or benefit from this intra-bank transfer, nor did she receive any notice of it. Consumer A had retired a few months earlier and the $70,000 was most of her savings. As a result, Consumer A's checking account had a balance of $84,542.63.

128. Account records further reflect that shortly thereafter, Citi accepted a $40,000 Payment Order and, in connection with that fraudulent Payment Orders, Citi executed a $40,000

EFT from Consumer A's Citi checking account, plus an EFT for a $17.50 fee. Consumer A did not make, authorize, or benefit from either the Payment Order or the EFTs.

129. After discovering that $40,017.50 had been removed from her account, Consumer A immediately called Citi. After a long hold, Defendant's representative, hearing Consumer A's story, transferred her to the fraud prevention department. After another long hold, Defendant's representative instructed Consumer A to travel to her local branch.

130. On information and belief, Consumer A's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $40,000 in stolen funds frozen or recalled.

131. The next morning, Consumer A went to her local branch but found it closed.

132. On the next business day, Consumer A again traveled to her local branch. The branch representatives were not helpful and did not know what number to call to contact the appropriate Citi department for assistance. The branch manager told Consumer A: "We don't handle these things." Eventually, Defendants' representative instructed Consumer A to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did.

133. That same day, Consumer A filed a police report at her local precinct.

134. A few days later, Consumer A called Citi customer service, and eventually was transferred to the fraud prevention department. The fraud prevention representative stated that Citi had not received the affidavit. Consumer A faxed in another copy of the affidavit.

135. Over the next several weeks, Consumer A called Citi customer service repeatedly to inquire on the status of the investigation. During each call, Consumer A was required to repeat her entire story. On at least one of the calls, Defendant's representative stated that a supervisor had approved Consumer A's claim and that she would receive her stolen funds back.

136. Citi subsequently sent Consumer A a December 15, 2021 letter stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer A was never interviewed in connection with any investigation by Defendant.

137. Citi subsequently rejected Consumer A's appeal of the denial of her claim.

138. As of the execution date of this Complaint, Consumer A has not received any of the $40,000 payment or $17.50 fee taken by Citi via EFTs from her account, or interest.

139. Consumer B. Consumer B has been a Citi bank account holder for decades. She does not recall ever sending a Payment Order to Citi.

140. On the evening of March 1, 2022, Consumer B received a communication from a scammer posing as Citi. The scammer stated that Consumer B's Citi bank account was locked and that she would not receive her direct deposit from her employer unless she verified certain personal information on file with Citi. Consumer B responded by providing the requested personal information, believing it was necessary to receive her next direct deposit.

141. Two days later, on March 3, 2022, at 2:00 p.m., Consumer B's home phone rang. She picked up and heard an automated prompt describe a $22,000 wire transfer and request that Consumer B confirm or deny the legitimacy of the transaction. Consumer B pressed the number on her phone to deny the legitimacy of the transaction. She was then placed on hold.

142. Defendant's representative eventually came on the line and Consumer B's husband stated that the $22,000 transaction was not legitimate. Defendant's internal records of this call state: "Client reported fraudulent wire transaction for $22,000."

143. Defendant's internal records reflect that at 2:02 p.m., while Consumer B was on hold, a scammer contacted Citi directly from a phone number that is not associated with Consumer

B to authenticate the fraudulent Payment Order. According to those records, the scammer entered a phone number that did not match Consumer B's records. The scammer was told to hold for a representative but hung up the phone. The Payment Order was then put on hold.

144. Defendant's internal records further reflect that four minutes later, while Consumer B was still on hold, the scammer contacted Citi directly from a phone number that is not associated with Consumer B to authenticate the fraudulent Payment Order. This time the scammer entered a phone number that was a match and—despite Consumer B having pressed the denial on the phone, the scammer's prior authentication failure, and the scammer contacting Citi from a phone number that was not associated with Consumer B—Citi accepted the fraudulent Payment Order.

145. Account records reflect that at 2:10 p.m. on March 3, 2022, Citi accepted a $22,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $22,000 EFT from Consumer B's bank account, leaving it with a near-zero balance. Consumer B did not make, authorize, or benefit from either the Payment Order or the EFT.

146. At 2:16 p.m., six minutes after Citi accepted the fraudulent Payment Order and while her husband was still on the phone, Consumer B logged onto her email account and discovered that in less than one hour before the phone call from Citi the scammer had changed her electronic banking password, added a new payee, enrolled her account in online wire transfer services, and, at 1:59 p.m., electronically sent the $22,000 Payment Order.

147. In response to a 1:59 p.m. "Fraud Alert" email asking her to let Citi "know immediately if you, or anyone you authorized, used your Citibank Checking account" to send a $22,000 Payment Order, Consumer B clicked on the button denying the legitimacy of the Payment Orders. Defendant's internal records state: "Activity denied via email."

148. Despite being informed of the fraudulent Payment Order by telephone and email on March 3, 2022, Citi did not contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $22,000 in stolen funds frozen or recalled until nearly three weeks later.

149. Concerned that Defendant's representative could not assist them over the phone, Consumer B and her husband hung up the phone and traveled together to their local branch. A branch representative contacted Citi fraud prevention to report the fraudulent online activity. The fraud prevention representative stated that the unauthorized transaction had been marked as cancelled, explained that new accounts should be opened, and represented to Consumer B that the $22,000 would be deposited into those new accounts within 24 to 48 hours. Defendant's internal records of this call state: "Wire noted as cancelled, funds should crdt back to the acct."

150. The next day, Friday, March 4, 2022, the branch representative contacted Consumer B and stated that the $22,000 had not yet been deposited into her account. Defendant's representative told Consumer B to check on the status of the funds the following week.

151. On March 7, 2022, Consumer B returned to the branch and Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. Defendant's representative told Consumer B that Citi had not opened any investigation and that Citi would not do so until the affidavit was completed.

152. Citi subsequently sent Consumer B an April 18, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Consumer B was never interviewed in connection with any investigation by Citi.

153. Consumer C. Consumer C has been a Citi bank account holder for many years.

154. In December 2021, a mortgage servicing firm that serviced loans, including a loan held by Consumer C, experienced a security incident. As a result, an unknown third party obtained personal identifying information, including name, address, loan information, and social security numbers for individuals with loans the firm serviced.

155. Account records reflect that three months later, on March 31, 2022, a scammer electronically transferred $1,887, $4,000, and $10,000 from three of Consumer C's checking and savings accounts to a checking account belonging to Consumer C. Consumer C did not make, authorize, or benefit from these intra-bank transfers, nor did he receive any notice of them. As a result, one of Consumer C's checking accounts had a balance of $38,763.27.

156. Account records reflect that, shortly thereafter, Citi accepted a $37,700 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $37,700 EFT from Consumer C's checking account, plus an EFT for a $25 fee, leaving it with a near-zero balance. Consumer C did not make, authorize, or benefit from either the Payment Order or the EFTs.

157. Four days later, on April 4, 2022, Consumer C received a letter from the mortgage servicing firm advising him of the security incident and stolen information.

158. Citi subsequently sent Consumer C an April 18, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Citi subsequently rejected Consumer C's appeal of the denial of his claim.

159. Consumer D. Consumer D has been a Citi bank account holder for twenty-seven years. He does not recall ever sending a Payment Order to Citi.

160. On April 4, 2022, Consumer D received a text message from "citi" stating that he needed to verify certain information. The message contained a link that he clicked.

161. The next day, April 5, 2022, Consumer D's phone rang. He picked up and Defendant's representative asked Consumer D to confirm or deny the legitimacy of a $44,440 wire transfer involving his Citi bank account. Consumer D denied the legitimacy of the transaction. The representative told Consumer D not to worry, that the funds were still in his account, and that Consumer D should travel to a local branch to transfer his funds into new accounts.

162. Defendant's internal records reflect that a scammer accessed Consumer D's mobile banking using a device that Citi had never seen, changed Consumer D's electronic password, and then electronically sent a fraudulent Payment Order. Those records also reflect that Citi assigned a risk score of 1,000 to the scammers' acts (as compared to scores of 1, 33, and 53 for Consumer D's prior usage), flagging risk factors that included a new device, recently linked devices, new IP addresses, login anomalies, and logins large distances from known locations.

163. Despite these red flags and Consumer D's own denial of the legitimacy of the wire transfer, while Consumer D was on the phone with Defendant's representative, the scammer contacted Citi directly to authenticate the fraudulent Payment Order. In violation of protocol, Citi accepted a $44,440 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $44,440 EFT from Consumer D's savings account, leaving it with a near-zero balance. Consumer D did not make, authorize, or benefit from either the Payment Order or the EFT.

164. When Consumer D subsequently visited his local branch, he discovered for the first time that $44,440 had been stolen from his bank account. Defendant's representative instructed Consumer D to execute and notarize an Affidavit of Unauthorized Online Wire Transfer to initiate an investigation. Defendant's representative completed the text of the affidavit for Consumer D, including a written submission stating: "Client received a fraudulent text message that contained a link. Client clicked on the link, allowing his phone to be compromised."

165. Citi subsequently sent Consumer D an April 29, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place." Consumer D was never interviewed in connection with any investigation by Citi.

166. Citi subsequently rejected Consumer D's appeal of the denial of his claim.

167. In June 2023, more than a year later and only after Plaintiff's involvement with Consumer D's matter, Defendant reimbursed Consumer D's bank account with $44,440.

168. Consumer E. Consumer E has been a Citi bank account holder for nearly twenty years. She does not recall ever sending a Payment Order to Citi.

169. On or around April 13, 2022, Consumer E received a text message that appeared to be from Citi. Consumer E clicked the link but did not take any further action.

170. The next day, April 14, 2022, at approximately 12:30 p.m., Consumer E's mobile phone began acting up and it was no longer able to access the mobile network.

171. Later that day, Consumer E logged onto her email account and learned that in the span of less than 30 minutes a scammer had upgraded Consumer E's online account status, enrolled in online wire transfer services, and electronically sent a $50,000 Payment Order to Citi.

172. Account records reflect that on April 14, 2022, Citi accepted a $50,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $50,000 EFT from Consumer E's checking account, leaving it with a near-zero balance. Consumer E did not make, authorize, or benefit from either the Payment Order or the EFT.

173. In response to a 2:01 p.m. "Fraud Alert" email asking her to let Citi "know immediately if you, or anyone you authorized, used your Citibank Checking account" to initiate a $50,000 wire transfer, Consumer E denied the legitimacy of the transaction.

174. After responding to the email, Consumer E called Citi customer service and was placed on a lengthy hold. Defendant's representative, after hearing Consumer E's story, responded that the stolen funds had "already left your account." When Consumer E's boss, who was participating on the call with her permission, asked whether the fraudulent transaction could be reversed, Defendant's representative refused to answer. Defendant's representative then instructed Consumer E to contact Citi's fraud prevention department.

175. Consumer E called the fraud prevention department number and, after another lengthy hold, explained to Defendant's representative that the unauthorized transaction was fraudulent. Defendant's representative instructed Consumer E to visit her local branch.

176. On information and belief, Consumer E's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $50,000 in stolen funds frozen or recalled.

177. Consumer E later visited her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. The affidavit stated that Consumer E's "phone was hack[ed]," among other details.

178. Consumer E also completed a police report at her local precinct.

179. Citi subsequently sent Consumer E a May 11, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

180. Citi subsequently rejected Consumer E's appeal of the denial of her claim.

181. As of the execution date of this Complaint, Consumer E has not received any of the $50,000 payment taken by Citi via EFT from her account, or interest.

182. Consumer F. Consumer F has been a Citi bank account holder for many years. He does not recall ever sending a Payment Order to Citi.

183. On April 28, 2022, Consumer F received a text message from "citi" stating that his information had not been verified in some time and that his account access "will be disabled unless we have verified" the information. The message contained a link to a website so that Consumer F could "sign on for a safe and secure banking experience."

184. Consumer F clicked on the link and was taken to a website that appeared to be a legitimate Citi website. The website contained the three security questions that Consumer F had answered when setting up online banking with Citi. Believing that this was a legitimate inquiry from Defendant, Consumer F answered the three questions and closed the website.

185. The next day, April 29, 2022, at 1:02 p.m., Consumer F's phone rang. He picked up and heard an automated prompt describe a $7,750 wire transfer and request that Consumer F confirm or deny the legitimacy of the transaction. Defendant's internal records reflect that Consumer F pressed "3" to deny the legitimacy of the transaction. Those records also reflect that Consumer F was told he would be connected to a "fraud specialist" and placed on hold.

186. Defendant's internal records reflect that while Consumer F was on hold, a scammer contacted Citi directly from a phone number that is not associated with Consumer F to authenticate the $7,750 Payment Order and that Citi accepted the fraudulent Payment Order.

187. Account records reflect that at 1:09 p.m. on April 29, 2022, Citi accepted a $7,750 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $7,750 EFT from Consumer F's checking account, leaving it with a balance of less than $75. Consumer F did not make, authorize, or benefit from either the Payment Order or the EFT.

188. Defendant's internal records also reflect that the scammer electronically sent the fraudulent Payment Order at 12:56 p.m. One minute later, Defendant sent a text message and email to Consumer F requesting verification of the transfer.

189. Consumer F first saw the text message from Defendant while still on hold following the automated call. The text message referred to a $7,750 transaction and Consumer F became concerned that either he had not stopped the fraudulent online activity by pressing 3 on his phone or that the automated call itself might be fraudulent. Consumer F hung up the phone and called the Citi customer service line on the back of his debit card. After a hold of approximately 50 minutes, Defendant's representative, after hearing Consumer F's story, stated that Citi should be able to stop the unauthorized transaction and instructed Consumer F to visit his local branch.

190. Defendant's internal records reflect that at 2:29 p.m. that same day, Consumer F first opened Defendant's "Fraud Alert" email requesting verification of the transaction and that he immediately "confirmed fraud." Those records also reflect that Citi took no action in response to this email response because "case status is resolved"—*i.e.*, the fraudulent Payment Order had already been accepted by Citi. Despite the telephonic denial, the notice of fraud by phone, and the email denial, Citi took no steps to contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $7,750 in stolen funds frozen or recalled for several hours.

191. Consumer F traveled to his local branch. Defendant's representative instructed him to execute and notarize an Affidavit of Unauthorized Wire Transfer, which he did.

192. Consumer F contacted Citi multiple times per week for the next several weeks but did not receive any updates on his stolen funds. Finally, on or around May 17, 2022, Defendant's representative informed Consumer F that Citi never received an affidavit.

193. That same day, Consumer F again traveled to his local branch to execute and notarize another affidavit, which he submitted along with a written dispute.

194. Weeks later, Citi sent Consumer F a letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

195. Citi subsequently rejected Consumer F's appeal of the denial of his claim.

196. In June 2023, more than a year later and only after Plaintiff's involvement with Consumer F's matter, Defendant reimbursed Consumer F's bank account with $7,750.

197. Consumer G. Consumer G has been a Citi bank account holder for decades.

198. On April 29, 2022, Consumer G received a text message that purported to be from Citi. The text message stated that fraudulent activity had been identified on Consumer G's Citi account and asked him to click a link to review the activity. Consumer G clicked the link, his phone began acting up, and it was no longer able to access the mobile network.

199. Email and account records reflect that, shortly after Consumer G's phone began acting up on April 29, 2022, and in the span of less than an hour, a scammer upgraded Consumer G's online account status, enrolled in online wire transfer services, and electronically transferred $9,000 from his savings account to his checking account. As a result of this intra-bank transfer, Consumer G's checking account had a balance of just over $27,000. Consumer G did not make, authorize, or benefit from this intra-bank transfer, nor did he receive any notice of it.

200. Defendant's internal records reflect that, an hour later, the scammer electronically sent three Payment Orders using Consumer G's savings account for $75,000, $75,000, and $68,000 to Citi. Together, had these Payment Order been accepted and had Citi executed EFTs in the same amounts, the unauthorized EFTs would have nearly emptied Consumer G's savings account.

201. Defendant's internal records further reflect that Citi sent "Fraud Alert" emails to Consumer G requesting verification of the Payment Orders. Those records also reflect that the scammer fraudulently authenticated one of the $75,000 Payment Orders by illicitly accessing Consumer G's email app on his hacked phone but did not respond to the "Fraud Alert" emails for the other $75,000 Payment Order or the $68,000 Payment Order.

202. Account records reflect that at 2:05 p.m. on Friday, April 29, 2022, shortly after the SIM swap, Citi accepted a $75,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $75,000 EFT from Consumer G's savings account. Consumer G did not make, authorize, or benefit from either the Payment Order or the EFT.

203. Defendant's internal records reflect that, more than 90 minutes later, the scammer electronically sent two additional Payment Orders using Consumer G's savings account in slightly smaller amounts of $70,000 and $60,000, as replacements for the prior $75,000 and $68,000 Payment Orders that had not been executed. Citi then received a phone call from the scammer regarding these fraudulent Payment Orders that resulted in a suspicious caller referral. Citi's fraud prevention department reviewed the referral and rejected the Payment Orders.

204. Despite the suspicious call referral and block on Consumer G's savings account, Citi did not place a hold on Consumer G's checking account at the time, nor did Citi immediately contact the beneficiary bank in the prior fraudulent $75,000 Bank-to-Bank Wire.

205. Account records reflect that two hours later, at 6:05 p.m., Citi accepted a $27,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $27,000 EFT from Consumer G's checking account, leaving it with a near-zero balance. Consumer G did not make, authorize, or benefit from either the Payment Order or the EFT.

206. Less than an hour later, at approximately 6:30 p.m., Consumer G visited his mobile carrier's store. He was told that his SIM had been reassigned to a different mobile device without his authorization. Consumer G obtained a letter from his carrier confirming the SIM swap.

207. Shortly after his mobile phone's SIM was fixed, Consumer G received numerous text messages from Defendant referring to the two executed transactions and four attempted but unexecuted transactions that had occurred during the prior several hours.

208. Consumer G immediately contacted Citi's customer service line at the number on the back of his debit card. After a lengthy hold, Defendant's representative, after hearing Consumer G's story, transferred Consumer G to Citi's fraud prevention department.

209. After another hold, Defendant's representative stated that Consumer G's account had been "frozen," that the fraudulent transaction would not go through, and that no money had been lost. The representative instructed Consumer G to travel to his local branch.

210. The next business day, Monday, May 2, 2022, Consumer G traveled to his local branch where he discovered, for the first time, that two transactions had been executed using his accounts in the amounts of $75,000 and $27,000. At the branch, Defendant's representative told to Consumer G "not to worry" because the transactions were fraudulent.

211. Defendant's branch representative also instructed Consumer G to execute and notarize two Affidavits of Unauthorized Online Wire Transfer, which he did.

212. That same day, Consumer G completed a police report at his local precinct.

213. Despite being informed of the fraudulent activity by Consumer G on April 29, 2022, Defendant Citi did not contact the beneficiary banks in the Bank-to-Bank Wire to have either the $75,000 or $27,000 frozen or recalled until May 4, 2022, five days later.

214. Citi subsequently sent Consumer G two May 11, 2022 letters, each stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam."

215. Citi subsequently rejected Consumer G's appeals of the denials of his claims. Consumer G submitted his mobile carrier's letter in connection with those appeals.

216. After contact by Plaintiff's office regarding Consumer G's matter, Defendant acknowledged in writing that its suspicious caller referral should have resulted in the securing of Consumer G's checking account in addition to his savings account. In June 2023, and only after Plaintiff's involvement with the matter, Defendant reimbursed Consumer G's checking account with $27,000. As of the execution date of this Complaint, Consumer G has not received any of the $75,000 payment taken by Citi via EFT from his savings account, or interest.

217. Consumer H. Consumer H has been a Citi bank account holder for thirty-plus years. She does not recall ever sending a Payment Order to Citi.

218. On July 6, 2022, Consumer H reviewed her bank accounts with Citi and found a message stating that her account was suspended due to fraudulent activity and instructing her to call a phone number. Consumer H called the identified number and a scammer answered, stated that he was a representative of Citi, and identified himself as James.

219. The scammer told Consumer H that he would be sending her codes from Citi to verify certain account activity and asked Consumer H to read the codes to him over the phone. Over the next 90 minutes, the scammer used codes read by Consumer H, who believed she was providing codes to secure her Citi bank accounts and prevent fraudulent activity, to change Consumer H's electronic banking password and create a new payee. At no time during the phone call did either Consumer H or the scammer discuss any transfers of money.

220. The next day, July 7, 2022, Consumer H discovered that $35,000 had been stolen from her bank accounts when she checked her account balances online. She immediately contacted Defendant's customer service line and was placed on a lengthy hold. Defendant's representative, after hearing Consumer H's story, instructed her to visit her local branch.

221. Account records reflect that at 1:37 and 1:38 p.m. the prior day—while Consumer H was on the phone with the scammer—the scammer electronically transferred $3,544.18, $5,169.19 and $6,091.44 from three of Consumer H's savings accounts to her checking account, leaving each savings account with a $0 balance. Consumer H did not make, authorize, or benefit from these intra-bank transfers, nor did she receive any notice of them. As a result of the three intra-bank transfers, Consumer H's checking account had a balance of $36,031.95.

222. Defendant's internal records reflect that, about an hour after the scammer changed Consumer H's electronic banking password, the scammer electronically sent a $35,000 Payment Order to Citi. Those same records reflect that Citi attempted to verify the Payment Order by an automated phone call to Consumer H, which went unanswered. At 2:07 p.m., after Consumer H did not respond to the verification attempt, Citi rejected the $35,000 Payment Order.

223. Five minutes later, at 2:12 p.m., Citi's fraud prevention department called Consumer H and left a voicemail seeking to "confirm recent online activity." The voicemail did not reference the rejected Payment Order for $35,000 or the intra-bank transfers.

224. Defendant's internal records further reflect that, at 2:25 p.m., the scammer electronically sent an identical $35,000 Payment Order to Citi. Those same records also reflect that, in response, Citi attempted to verify the Payment Order by email and text message sent at 2:27 p.m. Consumer H has never seen any such email and phone records she obtained from her mobile carrier do not reflect any text messages sent or received at 2:27 p.m.

225. Account records reflect that, despite Defendant's prior inability to verify a $35,000 Payment Order or contact Consumer H by phone, at 2:29 p.m. on July 6, 2022, Citi accepted a $35,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $35,000 EFT from Consumer H's checking account, leaving it with a near-zero balance. Consumer H did not make, authorize, or benefit from either the Payment Order or the EFT.

226. Despite being informed of the fraudulent activity by Consumer H over the phone on July 7, 2022, Citi did not contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $35,000 in stolen funds frozen or recalled until July 8, 2022, a full day later.

227. After returning home from out of state, Consumer H traveled to her local branch. Defendant's representative instructed Consumer H to execute and notarize an Affidavit of Unauthorized Online Wire Transfer Activity, which she did.

228. Consumer H also completed a police report at her local precinct.

229. Approximately 60 days later, Citi sent Consumer H a September 15, 2022 letter stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer H was never interviewed in connection with any investigation by Citi.

230. Citi subsequently rejected Consumer H's appeal of the denial of her claim.

231. As of the execution date of this Complaint, Consumer H has not received any of the $35,000 taken by Citi via EFT from her account, or interest.

232. Consumer I. Consumer I has been a Citi bank account holder for nearly thirty years. She does not recall ever sending a Payment Order to Citi.

233. Consumer I is a retired senior subsisting on social security. In July of 2022, she had saved up approximately $15,613, which she kept in a Citi bank account.

234. In early July 2022, Consumer I received a text message about a package being sent by Federal Express. Consumer I was in fact awaiting a delivery, and she clicked the link provided in the text message. Consumer I was directed to a website where she filled in the requested information and then landed on a screen requesting a $3.00 fee payment, which she made.

235. Concerned that the text message may have been a scam, Consumer I contacted Citi and asked that her current debit card be cancelled and that a new one be sent.

236. On July 12, 2022, at or around 6:30 p.m. and shortly after receiving her new debit card, Consumer I received a phone call from a scammer claiming to be from Citi. The scammer stated that Consumer I was supposed to receive a new debit card, which made Consumer I believe the scammer was legitimate. The scammer then told Consumer I that a fraudulent charge had already been made using her new card and that her account needed to be secured.

237. At the scammer's request, Consumer I provided the card number to the scammer. The scammer then told her that she would receive a code from Citi to secure the account and asked her to read the code back. Consumer I received a code and read it back over the phone.

238. While on the phone with the scammer, Consumer I attempted to log into her Citi online account but was not able to do so. She then checked her email account and first saw emails from Citi confirming a password change and the addition of a new payee.

239. Consumer I immediately hung up the phone and called the Citi customer service number on the back of her phone. After a hold of approximately 30 minutes, a representative came on the line and Consumer I stated that her account had been taken over by a scammer, asked for the account balance, and requested that the account be blocked. Defendant's representative responded that the account balance was $15,613. Consumer I replied "great" and requested that the representative immediately block any account activity. Defendant's representative then replied

that he did not have the ability to block the account but would transfer Consumer I. Consumer I pleaded not to be transferred or be re-identified, but she was placed on hold.

240. Consumer I remained on hold for approximately 20 minutes while crying. Account records reflect that while on this hold—after having told Defendant's representative that a scammer had fraudulent infiltrated her electronic banking—Citi accepted a $15,000 Payment Order and, in connection with that fraudulent Payment Order, Citi executed a $15,000 EFT from Consumer I's bank account, leaving it with a near-zero balance. Consumer I did not make, authorize, or benefit from either the Payment Order or the EFT.

241. Defendant's representative who next came on the line stated: "Thank you very much for calling Citi how can I help you?" Consumer I immediately explained that a scammer had illicitly accessed her online or mobile banking and was trying to wire money. The representative responded that two or three attempts had been made and that "your wire just went out."

242. Consumer I demanded that Defendant's representative immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to freeze or recall the stolen funds. Defendant's representative responded that "we don't do that" and that Citi "has a procedure."

243. On information and belief, Consumer I's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have the $15,000 in stolen funds frozen or recalled.

244. Consumer I hung up and called the beneficiary bank directly. The beneficiary bank's representative told Consumer I that the bank could not take any action because she was not an account holder and the bank had not received any recall request from Citi.

245. Consumer I later traveled to her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did.

246. Citi later sent Consumer I an August 1, 2022 letter stating: "You did not take adequate steps to safeguard your account. This failure compromised the security of your account information and directly contributed to allowing the transaction(s) in question to take place."

247. In October 2022, and only after Plaintiff's involvement with Consumer I's matter, Defendant reimbursed Consumer I's bank account with $15,000, but without interest.

248. Consumer J. Consumer J has been a Citi bank account holder for thirty-plus years. She does not recall ever sending a Payment Order to Citi.

249. On August 11, 2022, Consumer J received a call on her mobile phone that displayed on her phone as Citi. When she answered, a scammer stated that he was a Citi representative and identified himself as Gerald. The scammer asked Consumer J whether she had attempted two transactions in Georgia, and Consumer J responded that she had not. The scammer stated that Consumer J's debit card would be cancelled and that a new debit card would be issued.

250. The scammer then suggested that Consumer J set up two-factor authentication for her account and offered to assist. Consumer J agreed, and the scammer stated that he would be sending her codes to verify certain account activity and asked Consumer J to read the codes over the phone. The scammer then used codes read by Consumer J to change her electronic banking password and electronically send three Payment Orders for $49,300, $49,200, and $48,800 to Citi. During the call, the scammer thanked Consumer J for being a Citi customer and identified a recent transaction at a local grocery store (a real transaction) as the likely source of the account hack. At no time did either Consumer J or the scammer discuss any transfers of money.

251. Defendant's internal records reflect that Citi attempted to verify the three fraudulent Payment Orders by making direct, personal contact with Consumer J, but that Citi was unable to make contact directly with Consumer J. Citi rejected the three Payment Orders.

252. Defendant's internal records further reflect that, after these rejected Payment Orders, the scammer changed the username for Consumer J's electronic banking.

253. Despite a change in password, three rejected Payment Orders, and a change in username, all in succession in a short period, account records reflect that later that same day the scammer submitted and Citi accepted two Payment Orders in the amounts of $9,800 and $9,700 and, in connection with those fraudulent Payment Orders, Citi executed two EFTs in those same amounts from Consumer J's bank accounts, leaving each account with a near-zero balance. Consumer J did not make, authorize, or benefit from either the Payment Orders or the EFTs.

254. Shortly before 10:30 a.m. the next day, August 12, 2022, Consumer J received a delivery from Federal Express but it did not include a new debit card. Because she had expected to receive a new card, Consumer J called Citi's customer service line shortly before 11:00 a.m. During this call, Consumer J described her interactions the prior day with the scammer and asked if a new debit card had gone out. After placing Consumer J on a hold, Defendant's representative stated that a new card had not gone out and told Consumer J that she "would handle it."

255. At no time during this call did Defendant's representative mention any change in password, any change in username, or the Payment Orders (either the three rejected Payment Orders or the two accepted and executed Payment Orders). Defendant has acknowledged in writing that this call should have prompted further inquiry by Citi but did not.

256. Following her call with Citi customer service, Consumer J separately contacted Defendant's fraud prevention number. After another lengthy hold, she again described her interactions the prior day with the scammer. Defendant's representative told Consumer J that transfers had been executed using her accounts and instructed her to travel to her local branch to close her accounts and open new accounts to avoid further losses.

257. Account records further reflect that on August 12, 2022, at 11:54 a.m. and 12:46 p.m.—after Consumer J's call describing the scam to Defendant's representative who could have seen three rejected Payment Orders, two accepted Payment Orders, and two large EFTs but said and did nothing—Citi accepted two Payment Orders in the amounts of $9,900 and $9,897 and, in connection with those fraudulent Payment Order, Citi executed two EFTs in those amounts from Consumer J's Citi bank accounts, leaving each with a near-zero balance. Consumer J did not make, authorize, or benefit from either the Payment Orders or the EFTs.

258. On information and belief, Consumer J's conversations with Defendant's two representatives did not cause Citi to immediately contact the beneficiary bank in the fraudulent Bank-to-Bank Wire to have any of the approximately $40,000 in stolen funds frozen or recalled.

259. That same day, August 12, Consumer J traveled to her local branch. Defendant's representative instructed her to execute and notarize an Affidavit of Unauthorized Online Wire Transfer, which she did. The affidavit stated that Consumer J supplied codes to a scammer.

260. On August 16, 2022, Consumer J completed a police report at her local precinct.

261. Nearly 60 days later, Citi sent Consumer J four October 7, 2022 letters, each stating: "Claim was denied due to the fraud reported was caused by providing customer account information or authorization for the transactions that were determined to be a scam." Consumer J was never interviewed in connection with any investigation by Defendant.

262. In March 2023, seven months later, only after Plaintiff's involvement with Consumer J's matter, and after initially denying that Consumer J spoke with Citi before Citi accepted the two August 12, 2022 fraudulent Payment Orders, Defendant reimbursed Consumer J's four bank accounts with $9,800, $9,700, $9,900 and $9,897, but without interest.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Unauthorized Debits)

263. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

264. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

265. Under the EFTA and Reg. E, Citi, in response to a notice of an unauthorized EFT, must conduct an investigation, provisionally credit a consumer's account if Citi does not complete the investigation within 10 days, and refund all lost amounts in excess of (i) $50 if notice was provided within two business days of the consumer becoming aware of the unauthorized transfer or (ii) $500 if notice was provided within sixty days of the consumer becoming aware of the unauthorized transfer. 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. § 1005.6(b). With the exception of these liability thresholds based on the timing of notice provided, "a consumer incurs no liability from an unauthorized electronic fund transfer." 15 U.S.C. § 1693g(e).

266. An EFT is any transfer that "is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C. § 1693a(7). An EFT is unauthorized when the EFT is "initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." *Id*. § 1693a(12).

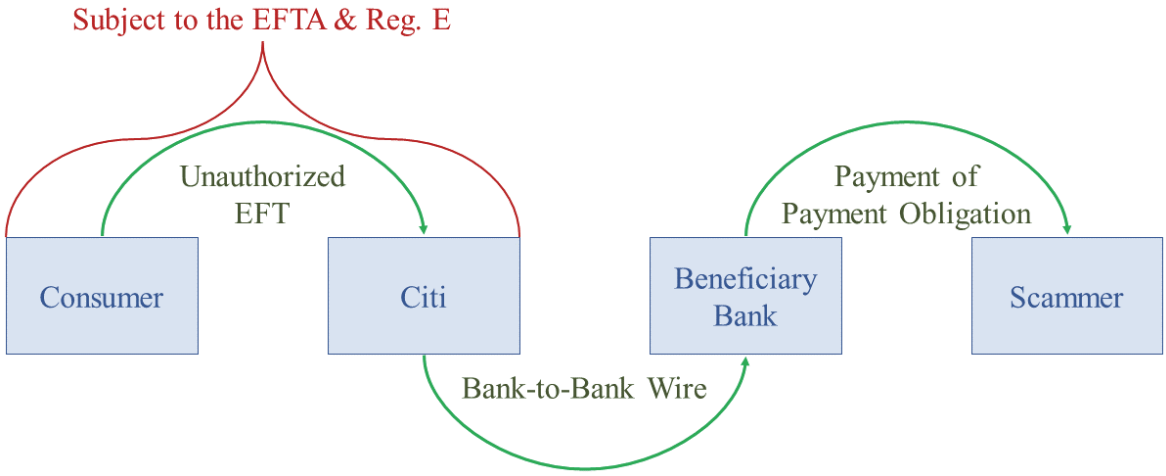
267. Citi has offered consumers online and mobile banking and has connected these services to wire transfer networks. As a result, Citi has provided consumers, through usernames and passwords, codes sent by text message, mobile apps, or a combination thereof, the ability to

electronically initiate wire transfers by sending Payment Orders directly to Citi, and the ability to fund those wire transfers by electronically authorizing Citi to debit their accounts.

268. Scammers have illicitly infiltrated New York consumers' online or mobile banking with Citi, including but not limited to those of Consumers A through J, and used this electronic access to wire transfer networks to send Payment Orders to Citi, which Citi accepted.

269. By sending fraudulent Payment Orders using computers or mobile devices, scammers have purported to electronically authorize Citi to debit consumers' bank accounts to pay itself for those Payment Orders, which Citi has done. Citi did not execute these debits by Fedwire, CHIPS, or means of any other service that transfers funds held at either Federal Reserve banks or depository institutions. Citi's electronic debits from consumers' accounts were EFTs.

270. Citi's execution of EFTs resulted from scammers having fraudulently infiltrated consumers' online or mobile banking and purporting to electronically authorize Citi to debit consumers' accounts without actual authority. Consumers have not benefitted from these EFTs. Citi's electronic debits from consumers' accounts were unauthorized EFTs:



271. Citi's handling of unauthorized EFTs initiated using compromised consumer online or mobile banking access has violated the EFTA and Reg. E in at least the following respects:

a. having required submissions of executed and notarized affidavits before investigating consumers' notices of unauthorized payment activity;

b. having failed to provisionally credit consumers' bank accounts within ten days of consumers' notices of unauthorized payment activity; and

c. having refused to reimburse consumers' bank accounts with the amount of stolen funds in excess of $50 or $500 where consumers provided notice of unauthorized payment activity within two or sixty business days of discovery, respectively.

272. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SECOND CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Unauthorized Intra-Bank Transfers)

273. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

274. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

275. Under the EFTA and Reg. E, Citi, in response to a notice of an unauthorized EFT, must conduct an investigation, provisionally credit a consumer's account if Citi does not complete the investigation within 10 days, and refund all lost amounts in excess of (i) $50 if notice was provided within two business days of the consumer becoming aware of the unauthorized transfer or (ii) $500 if notice was provided within sixty days of the consumer becoming aware of the unauthorized transfer. 15 U.S.C. §§ 1693f, 1693g; 12 C.F.R. § 1005.6(b). With the exception of these liability thresholds based on the timing of notice provided, "a consumer incurs no liability from an unauthorized electronic fund transfer." 15 U.S.C. § 1693g(e).

276. An EFT is any transfer that "is initiated through an electronic terminal, telephonic instrument, or computer or magnetic tape so as to order, instruct, or authorize a financial institution to debit or credit an account." 15 U.S.C. § 1693a(7). An EFT is unauthorized when the EFT is "initiated by a person other than the consumer without actual authority to initiate such transfer and from which the consumer receives no benefit." *Id*. § 1693a(12).

277. In advance of sending fraudulent Payment Orders, scammers have fraudulently infiltrated consumers' online or mobile banking to consolidate funds from multiple accounts into one account. Scammers have consolidated funds before sending Payment Orders to avoid needing to send multiple Payment Orders, thereby limiting the potential for consumers to notice and take action to stop fraudulent activity and limiting exposure to anti-fraud security measures. Citi's subsequent acceptance of fraudulent Payment Orders and execution of unauthorized EFTs resulted in losses of funds that would otherwise not have been available in the aggregate amount.

278. Scammers who have initiated intra-bank transfers did so electronically through online or mobile banking without authorization from consumers whose funds were in the accounts. These intra-bank transfers among consumers' accounts were unauthorized EFTs.

279. Citi's handling of unauthorized intra-bank EFTs in connection with fraudulent Payment Orders has violated the EFTA and Reg. E in at least the following respects:

a. having required submission of executed and notarized affidavits before investigating consumers' notices of unauthorized payment activity;

b. having failed to provisionally credit consumers' bank accounts within ten days of consumers' notices of unauthorized payment activity; and

c. having refused to reimburse consumers' bank accounts with the amount of stolen funds in excess of $50 or $500 where consumers provided notice of unauthorized payment activity within two or sixty business days of discovery, respectively.

280. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

THIRD CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(EFTA & Reg. E – Illegal Agreements)

281. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

282. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

283. The EFTA and Reg. E require banks who offer EFT services to consumers to disclose the terms and conditions of those services in "clear and readily understandable" language. 12 C.F.R. § 1005.4(a)(1); 15 U.S.C. § 1693c(a). The EFTA further provides that banks' terms and conditions cannot waive or alter the rights conferred by statute. 15 U.S.C. §1693l.

284. When consumers signed up for online or mobile banking with Citi they were required to agree to Defendant's online terms and conditions. The terms and conditions are adhesive and not subject to any negotiation between consumers and Citi.

285. Citi's online terms and conditions have violated the EFTA and Reg. E by failing to describe in clear and readily understandable terms the security protocols that Citi will actually deploy to prevent unauthorized EFTs initiated via online or mobile banking.

286. Citi's online terms and conditions also have violated the EFTA and Reg. E by altering federal consumer protections and rights in at least the following respects:

a. having improperly narrowed the scope of unauthorized EFTs by contractually defining any EFT initiated through online or mobile banking using usernames and passwords as an authorized EFT even if not made with actual authority;

b. having altered Citi's burden of proof by contractually providing that Citi may treat its own internal records and documents as conclusive evidence; and

c. having altered the scope of a reasonable investigation by Citi into notices of unauthorized EFTs provided to Citi by consumers.

287. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

FOURTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(UCC Violations)

288. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

289. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

290. Under Article 4-A of the UCC, Citi cannot refuse to refund payments for unauthorized Payment Orders unless Citi accepted the Payment Orders in good faith and in compliance with commercially reasonable security procedures and any instructions of its customers restricting acceptance of payment orders. U.C.C. § 4-A-202(2).

291. Citi has the burden of establishing that it is more probable than not that it acted in good faith and in compliance with the security procedures. U.C.C. § 4-A-105(g).

292. Under Article 4-A of the UCC, if Citi determines that its customers' funds were stolen in connection with unauthorized Payment Orders that were not enforceable, Citi "shall

refund any payment . . .and shall pay interest on the refundable amount calculated from the date the bank received payment to the date of the refund." U.C.C. § 4-A-204(1).

293. Citi has failed to employ commercially reasonable security procedures in connection with its handling of Payment Orders sent electronically in the following respects:

a. Citi's online terms and conditions have incorporated single-factor authentication protocols to verify Payment Orders sent electronically instead of layered security, including MFA, algorithmic monitoring of consumer and account behavior, mechanisms to identify high-risk transactions or anomalous behavior that trigger strengthened procedures, transaction limitations based on frequency, volume, and repeat activity, and training to ensure effective real-time responses to potential fraud, all of which are the hallmarks of commercially reasonable security procedures;

b. Citi has failed to materially alter and employ its most robust verification procedures and protocols in response to anomalous activity that should have indicated suspicious or fraudulent activity, including Payment Orders that: (i) were received within hours of changes to consumers' electronic banking passwords; (ii) were received within hours of changes in consumers' online account type or status; (iii) were received within hours of consumers first enrolling in online wire transfer services; (iv) would have, if accepted and Citi executed EFTs from consumers' accounts in the same amounts, resulted in a near-zero balances in consumers' bank accounts; (v) were received following intra-bank transfers from consumers' other bank accounts that left near-zero balances in those other bank accounts; (vi) were the first or one of the first ever sent by consumers after several years of account activity; and (vii) were received within hours of similar Payment Orders that had been cancelled or were unable to be verified; and

c. Citi has not had sufficient controls and has not trained employees to respond effectively in real-time to reject fraudulent Payment Orders in response to consumers' timely instructions to limit such activity. Specifically: (i) notices of fraudulent activity to Defendant's customer service representatives have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; (ii) long hold times on phone communications after consumers' notices of fraudulent activity have slowed consumers' efforts to secure accounts; (iii) notices of fraudulent activity via telephonic dial or email have not secured consumers' bank accounts such that scammers could no longer successfully execute fraudulent Payment Orders; and (iv) requirements to travel to local branches to secure accounts have left consumers' bank accounts vulnerable to scammers' fraudulent activity.

294. Citi has not acted in good faith or in compliance with its customers instructions in connection with its handling of Payment Orders sent electronically in the following respects:

a. Citi has accepted Payment Orders in the face of one or more of the red flags identified in the preceding paragraph, all of which are common indicators of potentially fraudulent activity that should trigger robust verification protocols;

b. Citi has accepted Payment Orders after consumers had provided notice that those Payment Orders were unauthorized and the result of fraudulent activity; and

c. Citi has substantially delayed contacting beneficiary banks to freeze or recall consumers' stolen funds after notice of fraudulent activity.

295. In addition, Citi's standard-form denial letters, which have appended no evidence, have described no findings, and have followed wholly inadequate investigations that often have not included basic interviews with affected consumers, have not satisfied Citi's burden to prove

that it was more probable than not that it (i) acted in compliance with security procedures, (ii) acted in good faith, or (iii) adhered to consumers' instructions regarding Payment Orders.

296. Finally, where Citi has determined that it was obligated to refund consumers under Article 4-A in connection with scammers' fraudulent Payment Orders, Citi has replaced the lost funds in consumers' bank accounts but often has not included any interest.

297. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

FIFTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(SHIELD Act & GBL § 349)

298. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

299. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

300. New York's SHIELD Act requires businesses that own or license computerized data that includes private information of New York residents, including financial account information, to develop, implement, and maintain reasonable safeguards to protect the security, confidentiality, and integrity of that private information. GBL § 899-bb(2). This includes, among other obligations, implementation of reasonable (i) administrative safeguards to both identify reasonably foreseeable internal and external risks and train and manage employees in its security program, *id*. §§ 899-bb(2)(b)(ii)(A)(2)–(4), and (ii) technical safeguards to detect, prevent, and respond to attacks or system failures, *id*. § 899-bb(2)(b)(ii)(B)(3).

301. Failure to comply with the SHIELD Act is deemed a violation of GBL § 349 and Plaintiff is empowered to bring an action on behalf of the People of New York to enjoin such violations and obtain civil penalties under GBL § 350-d. GBL § 899-bb(2)(d).

302. Citi owns or licenses computerized data that includes private information of New York residents, including financial account information belonging to Consumers A through J.

303. Citi has failed to adopt reasonable administrative and technical safeguards, and to identify and respond to the reasonably foreseeable risks posed by scammers accessing financial account information, including as to Consumers A through J. Citi has failed to adopt appropriate layered security, including MFA, algorithmic monitoring of consumer and account behavior, mechanisms to identify high-risk transactions or anomalous behavior that trigger strengthened procedures, or transaction limitations based on frequency, volume, and repeat activity.

304. Citi has failed to train and manage employees to respond to consumers' notice of fraudulent online or mobile banking access or unauthorized payment activity, including:

a. not training employees to secure bank accounts such that scammers could no longer engage in unauthorized activity following verbal notice over the phone;

b. not training employees to not place consumers on long telephonic holds following verbal notice over the phone;

c. not training employees to secure bank accounts such that scammers could no longer engage in unauthorized activity following electronic notice;

d. not training employees to reject all Payment Orders after consumers had provided notice that those Payment Orders were unauthorized and were the result of scammers fraudulent access to online or mobile banking; and

e. training employees to instruct consumers to travel to local branches to secure bank accounts such that scammers could no longer engage in unauthorized activity.

305. Citi has failed to implement technical safeguards to detect, prevent, and respond to either scammers' infiltration of online or mobile banking or scammers' fraudulent payment

activity, thereby compromising consumers' financial account information. Citi also has not responded effectively but instead has accepted large-dollar Payment Orders following anomalous account activity, including (i) changes to consumers' usernames or passwords; (ii) changes in consumers' online account type or status; (iii) enrollments in online wire transfer services; and (iv) transfers from consumers' other bank accounts that left near-zero balances in those accounts.

306. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SIXTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(Red Flag Rule)

307. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

308. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

309. The Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 rule (the "Red Flag Rule") is a joint final rule adopted on November 9, 2007 by, among other federal agencies, the Federal Trade Commission, 16 C.F.R. § 681.1, and the Office of the Comptroller Currency, 12 C.F.R. § 41.90.

310. The Red Flag Rule applies to "financial institutions," which is defined by reference to the federal Consumer Credit Protection Act, 15 U.S.C. § 1681 *et seq*. 16 C.F.R. § 681.1(b)(7); 12 C.F.R. § 41.90(b)(7). The term "financial institution" means a State or National bank, a State or Federal savings and loan association, and other enumerated entities. 15 U.S.C. § 1681a(t).

311. The Red Flag Rule applies to covered accounts, which are accounts that financial institutions offer or maintain, primarily for personal, family, or household purposes, that involve

or are designed to permit multiple payments or transactions, including checking accounts and savings accounts. 16 C.F.R. § 681.1(b)(3)(i); 12 C.F.R. § 41.90(b)(3)(i).

312. The Red Flag Rule requires financial institutions that offer or maintain covered accounts to establish an identity theft prevention program that is designed to detect, prevent, and mitigate identify theft, including the detection and appropriate response to Red Flags, 16 C.F.R. § 681.1(d)(2)(ii)–(iii); 12 C.F.R. § 41.90(d)(2)(ii)–(iii), and to ensure that the identity theft prevention program is periodically updated to reflect changes in risks to customers posed by identify theft, 16 C.F.R. § 681.1(d)(2)(iv); 12 C.F.R. § 41.90(d)(2)(iv).

313. A Red Flag is a pattern, practice, or specific activity that indicates the possible existence of identity theft. 16 C.F.R. § 681.1(b)(9); 12 C.F.R. § 41.90(b)(9).

314. Citi is a financial institution subject to the Red Flag Rule. Citi offers and maintains covered accounts, including accounts belonging to Consumers A through J.

315. Citi has failed to ensure that Defendant's identify theft prevention program detects and responds appropriately to Red Flags in at least the following respects:

a. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of changes to consumers' electronic banking passwords;

b. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of changes in consumers' online account type or status;

c. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted within hours of consumers first enrolling in online wire transfer services;

d. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that would have, if Citi executed EFTs from consumers' accounts in the same amounts, resulted in a near-zero balances in consumers' bank accounts;

e. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted after transfers from consumers' other bank accounts that left near-zero balances in those other bank accounts;

f. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were received within hours of similar Payment Orders that had been cancelled or were unable to be verified;

g. not detecting as Red Flags or responding appropriately to prevent large-dollar Payment Orders that were electronically transmitted in connection with multiple Red Flags identified in the preceding subparagraphs; and

h. not responding appropriately to mitigate financial and other harms caused by identity theft in response to Red Flags identified in any preceding subparagraphs.

316. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

SEVENTH CAUSE OF ACTION
Executive Law § 63(12) (Fraud)

317. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

318. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent fraud in the carrying on, conducting, or transaction of business in the state of New York.

319. Citi has engaged in fraudulent practices in its account administration and handling of unauthorized EFTs and Payment Orders sent electronically in at least the following respects:

a. having enticed consumers to enroll in online and mobile banking by stressing the security of electronic banking and by creating the impression that online and mobile banking were no less secure than in-person banking when in fact enrollment in online or mobile banking resulted in less security, including adoption of security procedures for Payment Orders sent electronically that did not rely on direct, personal verification but instead employed a single-factor verification mechanism and which permitted Citi, at its sole discretion, to choose from other weak security procedures (or none) that did not effectively defeat unauthorized Payment Orders;

b. having misrepresented consumers' rights and obligations with respect to unauthorized EFTs, including by failing to immediately investigate notices of unauthorized EFTs and failing to provisionally credit consumers' bank accounts;

c. repeatedly having represented that bank accounts were secure and directing consumers to visit local branches when in fact the bank accounts were not safe from scammers, Defendant's representatives often did not secure or even have the ability to secure consumers' accounts, and scammers retained the ability to access online or mobile banking and successfully send fraudulent Payment Orders electronically by satisfying alternative security procedures;

d. having required consumers who provided notice of unauthorized EFTs to execute affidavits asserting claims for unauthorized wire transfers;

e. repeatedly having told consumers that no action could be taken, including any investigation, unless consumers executed affidavits;

f. having encouraged consumers to complete affidavits that describe the circumstances that led to scammers illicitly accessing online or mobile banking under the

pretense of needing affidavits to initiate investigations to recover consumers' funds, at a time when consumers were under severe duress, but then used information provided by consumers to deny consumers' fraud claims;

g. having not immediately attempted to recall funds sent to beneficiary banks following notice of fraudulent activity, delaying for days or even weeks, often after having indicated that funds lost as a result of fraud would be returned; and

h. having represented in its standard form denials for what Citi misleadingly refers to as "unauthorized online wire transfers" that consumers acted improperly—such as not taking "adequate steps to safeguard" accounts or "providing customer account information" in responses to scams—as bases to deny any obligation by Citi to reimburse, which falsely led consumers to believe that their own actions were relevant and deprived them of their legal rights to recover stolen funds.

320. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent fraudulent conduct in violation of Executive Law § 63(12).

EIGHTH CAUSE OF ACTION
Executive Law § 63(12) (Illegality)
(GBL § 349)

321. Plaintiff repeats and realleges the allegations in paragraphs 1 to 262 above.

322. New York's Executive Law § 63(12) authorizes Plaintiff to seek injunctive and other equitable relief when any individual or business engages in repeated and persistent illegal conduct in the carrying on, conducting, or transaction of business in the state of New York.

323. New York's General Business Law prohibits deceptive acts and practices in the conduct of any business, trade, or commerce in the state of New York. GBL § 349(a).

324. Citi has engaged in deceptive practices in its account administration and handling of unauthorized EFTs and Payment Orders sent electronically in at least the following respects:

a. having enticed consumers to enroll in online and mobile banking by stressing the security of electronic banking and by creating the impression that online and mobile banking were no less secure than in-person banking when in fact enrollment in online or mobile banking resulted in less security, including adoption of security procedures for Payment Orders sent electronically that did not rely on direct, personal verification but instead employed a single-factor verification mechanism and which permitted Citi, at its sole discretion, to choose from other weak security procedures (or none) that did not effectively defeat unauthorized Payment Orders;

b. having misrepresented consumers' rights and obligations with respect to unauthorized EFTs, including by failing to immediately investigate notices of unauthorized EFTs and failing to provisionally credit consumers' bank accounts;

c. repeatedly having represented that bank accounts were secure and directing consumers to visit local branches when in fact the bank accounts were not safe from scammers, Defendant's representatives often did not secure or even have the ability to secure consumers' accounts, and scammers retained the ability to access online or mobile banking and successfully send fraudulent Payment Orders electronically by satisfying alternative security procedures;

d. having required consumers who provided notice of unauthorized EFTs to execute affidavits asserting claims for unauthorized wire transfers;

e. repeatedly having told consumers that no action could be taken, including any investigation, unless consumers executed affidavits;

f. having encouraged consumers to complete affidavits that describe the circumstances that led to scammers illicitly accessing online or mobile banking under the

pretense of needing affidavits to initiate investigations to recover consumers' funds, at a time when consumers were under severe duress, but then used information provided by consumers to deny consumers' fraud claims;

g. having not immediately attempted to recall funds sent to beneficiary banks following notice of fraudulent activity, delaying for days or even weeks, often after having indicated that funds lost as a result of fraud would be returned; and

h. having represented in its standard form denials for what Citi misleadingly refers to as "unauthorized online wire transfers" that consumers acted improperly—such as not taking "adequate steps to safeguard" accounts or "providing customer account information" in responses to scams—as bases to deny any obligation by Citi to reimburse, which falsely led consumers to believe that their own actions were relevant and deprived them of their legal rights to recover stolen funds.

325. By reason of the conduct alleged herein, Defendant has engaged in repeated and persistent illegal conduct in violation of Executive Law § 63(12).

DEMAND FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court issued an order and judgment under Executive Law § 63(12) and General Business Law § 349:

a. permanently enjoining Defendant, its agents, trustees, employees, successors, heirs, and assigns; and any other person under their direction or control, whether acting individually or in concert with others, or through any corporate or other entity or device through which one or more of them may now or hereafter act or conduct business, from engaging in the fraudulent and illegal practices alleged herein;

b. ordering Defendant to provide an accounting of all consumers whose claims for monetary losses in connection with unauthorized Payment Orders and debit authorizations were denied by Defendant in the last six years;

c. appointing an independent third party paid for by Defendant to review the accounting to identify every consumer who was harmed by Defendant's fraudulent and illegal practices alleged herein;

d. ordering Defendant to provide restitution and damages to all injured consumers, whether known or unknown, at the time of the decision and order;

e. ordering Defendant to disgorge all profits from the fraudulent and illegal practices alleged herein;

f. directing Defendant, under General Business Law § 350-d, to pay a civil penalty of $5,000 to the State of New York for each violation of General Business law § 349;

g. awarding to Plaintiff, under CPLR 8303(a)(6), costs in the amount of $2,000; and

h. granting such other and further relief as the Court deems just and proper.

Dated: January 30, 2024

Respectfully submitted,

LETITIA JAMES
Attorney General of the State of New York

By: */s/ Christopher L. Filburn*
Christopher L. Filburn
Assistant Attorney General
Bureau of Consumer Frauds & Protection
28 Liberty Street, 20th Floor
New York, New York 10005
Tel.: 212.416.8303
Email: christopher.filburn@ag.ny.gov

Of counsel:

Jane M. Azia
Bureau Chief

Laura J. Levine
Deputy Bureau Chief