EXHIBIT N

REDACTED

EXHIBIT N

FILED PROVISIONALLY UNDER SEAL WITH REDACTIONS PURSUANT TO STIPULATED PROTECTIVE ORDER

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA

IN RE BANK OF AMERICA CALIFORNIA UNEMPLOYMENT BENEFITS LITIGATION	Case No. 3:21-md-02992-GPC-MSB

EXPERT REBUTTAL REPORT OF NATALIE LOEBNER

April 4, 2025

26. For the reasons stated below, CFF-1 was not a reasonable use of an automation as it fell woefully short of meeting industry standards to be reasonably tailored to minimize collateral damage to innocent cardholders which the Bank knew about. In my opinion, the unreasonable approach by the Bank at each stage of the CFF-1 development, implementation, and effectiveness measurement demonstrates this was a flawed automation from start to finish.

A. In developing and implementing CFF-1 automation, the Bank failed to consider well-known situations such as card skimming—a pervasive crime where a cardholder's PIN is compromised, enabling unauthorized cash withdrawals from an ATM—where a claimant cardholder would be a true victim.

27. [redacted][11] In my experience, it is highly problematic to rely on automations that are not reasonably tailored for the specific use case. Assessing whether CFF-1—or any rule—is reasonably tailored to achieve its desired objective requires assessing that rule's underlying presumptions. By categorically denying any unauthorized-transaction claim based on a PIN-enabled ATM cash withdrawal, CFF-1 treats such claims as inherently

[11] Cronan Rep., ¶16, Pesce Rep., ¶¶23, 24, and 55.

fraudulent. [redacted]

28. One of the more obvious and notorious examples of a valid unauthorized-transaction claim in which EDD funds were stolen from a cardholder at an ATM involves card-skimming. Based on my experience supporting financial crime investigations, I am familiar with card skimming operations. Card skimming occurs when criminals compromise payment terminals or ATMs by installing card-reading devices. The cardholder's PIN can be compromised using different techniques, including pinhole cameras or keypad overlays. Criminals use information captured by a skimming device to generate a duplicate or cloned card to make unauthorized purchases or to make ATM withdrawals using the cardholder's compromised PIN. Card skimming has become so frequent an occurrence that the FBI, U.S. Secret Service, and other law enforcement agencies

[12] BANA_EDD_MDL-00004996 [redacted]

and regulators have issued public warnings and brought numerous card skimming cases.[13] These compromises have been known to occur at ATMs, gas stations, and other locations with publicly accessible terminals accepting debit cards with PIN input.[14] PIN inputs are generally required at non-ATM terminals where the card or terminal is not EVM chip-enabled.

29. Based on my experience engaging with financial institutions, card skimming is a risk with which banks issuing debit and prepaid cards are familiar, both before and during the COVID-19 pandemic. Financial institutions reduce this risk by implementing processes and procedures to detect and mitigate the risk of card skimming. Common measures to identify and mitigate card skimming risks include: (1) monitoring transactions to detect point-of-sale (POS) terminal usage

---

[13] The FBI Scams and Safety webpage, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-frauds-and-scams/skimming, cautions the public on the various techniques used to compromise cardholder PINs. Similarly, the U.S. Secret Service webpage, https://www.secretservice.gov/investigations/skimming, states the Service investigates hundreds of cases a year and advises that PIN compromise occurs at a variety of common merchants like pharmacies, gas stations, and grocery stores. The webpage also highlights the recommendation to use chip enabled cards to reduce the exposure of the cardholder's PIN as merchant locations. In 2018, the Federal Trade Commission (FTC) issued a consumer alert related to card skimming, https://consumer.ftc.gov/consumer-alerts/2018/08/watch-out-card-skimming-gas-pump. The Office of the Comptroller of the Currency (OCC) identifies advances in card skimming technology in its Fiscal Year 2018 Bank Supervision Operating Plan, https://www.occ.gov/news-issuances/news-releases/2017/nr-occ-2017-113a.pdf, and 2019 Fall Semiannual Risk Perspective, https://www.occ.gov/publications-and-resources/publications/semiannual-risk-perspective/files/pub-semiannual-risk-perspective-fall-2019.pdf.

[14] United States Secret Service, U.S. Secret Service Serves up Cold Dish of Justice to Gas Pump Skimmers, U.S. Secret Service Media (November 22, 2018), https://www.secretservice.gov/press/releases/2018/11/us-secret-service-serves-cold-dish-justice-gas-pump-skimmers (Press release regarding a nationwide initiative called Operation Deep Impact to combat the targeting of gas stations noting the identification of nearly 200 skimmers.)

that connects numerous cards to suspicious ATM withdrawal or purchase patterns; (2) physically inspecting ATMs to identify skimming devices; (3) proactively flagging transactions associated with compromised ATMs and POS terminals; and (4) leveraging skimming indicators placed on transactions to streamline transaction holds and cardholder engagement.[15]

30. It is my opinion that the Bank was aware of and treated card skimming as a risk before and during the Bank's deployment of CFF-1. My opinion is supported by records I reviewed in this case in which Bank employees expressly discussed card skimming. Further, the Bank was publicly highlighted in Department of Justice press releases during the relevant timeframe as either assisting law enforcement with card skimming investigations or otherwise acknowledging having customers as card-skimming victims.[16] Nonetheless, the

---

[15] BANA_EDD_MDL-00057505 (Email from Bradley Garfield on October 30, 2020, to John Denning and Ruchira Ghosh noting a handful of common transaction attributes financial institutions use to detect and address card skimming, although not incorporated into CFF-1).

[16] A sampling of DOJ press releases illustrative of the prevalence of the risk before and during the Class Period: Twelve Individuals Charged in ATM Skimming Conspiracy (November 16, 2016), https://www.justice.gov/archives/opa/pr/twelve-individuals-charged-atm-skimming-conspiracy (a 2016 case where skimming devices were found at Bank of America locations.); Romanian Citizen Pleads Guilty in ATM Skimming Conspiracy (March 29, 2017), https://www.justice.gov/archives/opa/pr/romanian-citizen-pleads-guilty-atm-skimming-conspiracy (a 2017 case identifying both Bank of America and PNC Bank customers as victims); Romanian National Sentenced for Multi-State ATM Card Skimming Scheme (June 3, 2019), https://www.justice.gov/archives/opa/pr/romanian-national-sentenced-multi-state-atm-card-skimming-scheme (a 2019 case noting keypad overlays as one of the ways PINs were compromised); Seven Members and Associates of Large-Scale Gas Pump Skimming Device Organization Charged with Racketeering and Money Laundering Conspiracies (May 8, 2024), https://www.justice.gov/archives/opa/pr/seven-members-and-associates-large-scale-gas-pump-

Bank failed to account for this scenario when implementing CFF-1 in its unauthorized-transaction claim process.

31. Card-skimming is one of the more notable examples in which a cardholder-claimant would be the victim rather than the fraudster and is a situation of which the Bank was well aware. In my opinion, a reasonable automated process would have accounted for this real and well-known scenario; however, CFF-1 did not take this into account.

B. Even if there was a potential correlation between fraud and an ATM cash withdrawal, it was unreasonable for the Bank to use this correlation alone in developing CFF-1.

32. The Bank's reliance on its CFF-1 as a stand-alone basis for denying unauthorized-transaction claims rests on the incorrect assumption that all unauthorized-transaction claims based on ATM/PIN cash transactions are inherently false and fraudulent. [redacted]

---

skimming-device-organization-charged (a 2024 case cover conduct from 2014 to 2024 involving large scale gas station skimming operations).

[17] Pesce Rep. ¶56 and Fn. 129; Cronan Rep.¶49.