Exhibit 160

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 JANE CLONINGER

IN SUPPORT OF PLAINTIFFS' MOTION FOR CLASS CERTIFICATION

November 21, 2024

TABLE OF CONTENTS

I. INTRODUCTION

1. I have been retained as an expert in *In re Bank of America California Unemployment Benefits Litigation*, Case No. 3-21-md-02992-GPC-MSB, by co-lead counsel for Plaintiffs, Cotchett, Pitre & McCarthy, LLP and Altshuler Berzon LLP (collectively, "Plaintiffs' Counsel"). I submitted my initial expert report to this Court in support of Plaintiffs' motion for class certification on August 29, 2024. Ex. 2 ("Cloninger Rep.").[1]

2. Plaintiffs' Counsel asked me to review and respond to opinions expressed in the Declaration of Pamela Joseph submitted by Defendant Bank of America, N.A. (the "Bank") in support of its opposition to Plaintiffs' motion for class certification. DX 4 ("Joseph Rep.").[2] Joseph was retained by the Bank to respond to my initial Cloninger Report, and this rebuttal report addresses those responses, as set forth in the Joseph Report.

3. In preparing this rebuttal report, I principally relied upon the knowledge, training, experience, and expertise I have developed throughout my 35-year career in the payments industry. I also considered documents, testimony, and information produced in discovery in this litigation as well as publicly available documents and information. The specific materials I considered are cited in this report and in the attached Appendix A.

4. My work on this case is ongoing, and I may review additional materials or conduct additional analysis. I reserve the right to update, refine, or revise my opinions as appropriate, including if additional information becomes available to me.

---

[1] My qualifications and hourly rate were disclosed in my original report and have not changed. I have no additional publications or testimony to disclose.

[2] "Ex." refers to exhibits to the Chan Declaration and Supplemental Chan Declaration in support of Plaintiffs' class certification ("Mot."); "DX" refers to exhibits to the Brys Declaration in support of the Bank's opposition to class certification ("Opp.").

II. SUMMARY OF OPINIONS

5. I have reviewed the Joseph Report and the sources cited therein. Nothing in the Joseph Report or the sources on which Joseph relies changes my opinions as expressed in the Cloninger Report, which I stand by and reaffirm. I believe that many of the opinions expressed in the Joseph Report are misleading, irrelevant, or unsupported by evidence, for the reasons set forth below.

6. The Joseph Report opines that "EMV chips do not prevent cards from being vulnerable to skimming, shimming, or other forms of information compromise," Joseph Rep. ¶14, and that skimming devices are "[redacted]" Joseph Rep. ¶37. These statements, while true at a broad level of generality, have little if anything to do with the opinions set forth in the Cloninger Report. Although the mag-stripe on an EMV chip card can be skimmed and a moment-in-time snapshot of an EMV chip can be "shimmed" as well, the crucial fact that Joseph ignores, which was critical to many of my opinions in the Cloninger Report, is that EMV chips create *dynamic data*, which make EMV chips nearly impossible to clone. *See infra*, §III.A. Without the dynamic component created by an EMV chip, a counterfeit card that has been created using only the information skimmed from a mag-stripe on an EMV chip card cannot be used to engage in fraudulent card-present transactions at a chip-enabled ATM except in narrow circumstances, as described *infra* ¶¶23-36. That is why *EMV chip cards provide strong protection against card-present counterfeit fraud*, as is widely recognized throughout the payments industry and in the Bank's own documents. By contrast, a skimmed "mag-stripe only" card, such as the EDD debit cards at issue in this case, can easily be cloned and used to make fraudulent card-present transactions, including unauthorized ATM withdrawals (because skimmers are typically used in conjunction with devices that capture the cardholder's PIN)—making EDD debit cardholders a

foreseeably attractive target for fraud during the pandemic. Cloninger Rep. ¶¶14(a), 14(d)-(f), 15-28. For these reasons, EMV chips are widely regarded as an industry standard security measure in payment cards—a critical point that Joseph does not dispute.

7. The Joseph Report opines that "[t]he addition of EMV chips to the EDD prepaid debit cards issued by the Bank would not have prevented many of the unauthorized transactions that were reported to the Bank," Joseph Rep. ¶15, and that "in order to determine whether an EMV chip would have prevented any of the unauthorized transactions reported to the Bank, one would have to look at the circumstances surrounding the transaction, including whether it was fraudulent, and where and how it was made," *id.* ¶16. To the extent the Joseph Report purports to be addressing the facts and circumstances of *this* case (which is limited to card-present ATM unauthorized-transaction fraud) and to the Cloninger Report I prepared to address those specific facts and circumstances, I disagree with those opinions. *See infra*, §III.B

(a) First, every class member in this case reported an unauthorized ATM withdrawal, which is necessarily a card-present transaction. For every class member who experienced an unauthorized ATM withdrawal, the most likely explanation is that the unauthorized transaction was committed by someone using a counterfeit card (and that the counterfeit card was most likely created through skimming combined with PIN capture, which gives the criminal access to the PIN as well as personal card data). Again, for the reasons I previously explained, EMV chips are extremely effective at preventing card-present counterfeit fraud. Because nearly all ATMs in the U.S. had chip readers by 2020-2021 and because all of Bank of America's own ATMs had chip readers during that period, the addition of EMV chips to EDD debit cards would have prevented all or nearly all of the unauthorized ATM withdrawals that class members reported and that are at issue in this litigation.

(b) Second, the addition of EMV chips to EDD debit cards also would have been highly effective at preventing any additional unauthorized card-present point-of-sale ("POS") transactions, which I understand some class members may have reported in addition to an unauthorized ATM withdrawal ("[redacted]"[3])—even though what the Bank describes as [redacted] by definition include [redacted].

(c) The transactions described by Joseph, in which a transaction is made with an EMV chip-enabled card yet the chip is not required to be read (either because the ATM or POS terminal is not enabled with an EMV chip reader or because the chip is not functional, as further described *infra*) do not detract from these conclusions. Any such "fallback" transactions (i.e., where the EMV chip cannot be read, requiring the ATM or vendor to fall back to relying only on the mag-stripe for card security) attempted with a counterfeit copy of a Bank-issued EMV chip card would have triggered additional security rules, such as secondary authentication and strict withdrawal limits, if the Bank provided EDD cardholders the same anti-fraud protections it provided its non-prepaid consumer debit cardholders. Fallback transactions are also subject to industry controls to limit their frequency. Joseph posits two other types of infrequent fraud that could possibly have led to an unauthorized transaction and that EMV would not have prevented—[redacted]. Joseph Rep. ¶¶67, 80. Based on my extensive professional experiences and the sources cited in this report, neither of these two types of card-present fraud is likely to account for any significant

[3] *See* Ex. 50 at -90640, -90643; Ex. 17 (Letson Tr.) 92:19-23.

percentage of the transactions reported by the class. For these reasons and others stated in the Cloninger Report and below, it continues to be my view that EMV chips would have prevented nearly all the unauthorized ATM transactions class members reported to the Bank and that the Bank denied solely because of Indicator 1 of the Bank's automated Claim Fraud Filter ("CFF-1").

(d) Other types of fraud addressed in the Joseph Report (such as enrollment fraud, first-party fraud, and fraudulent card-not-present transactions, e.g. online fraud) are entirely irrelevant to this case. Although the Joseph Report goes on at length about whether the presence of an EMV chip could have prevented these other types of fraud, that inquiry has nothing to do with this case or with the opinions stated in the Cloninger Report, whose scope was limited to the extent to which including EMV chips in the Bank's EDD debit cards would have prevented the specific types of unauthorized-transaction fraud at issue in this litigation: card-present ATM fraud that triggered the Bank's application of CFF-1. For purposes of my Report, it is entirely irrelevant whether adding EMV chips to the Bank's EDD debit cards would have prevented other types of fraud that are not at issue here.

8. The Joseph Report also opines that, "[i]n order to determine whether an EMV chip would have prevented access to or compromise of information on an EDD prepaid debit card, one would have to look at the circumstances surrounding the access or compromise. Joseph Rep. ¶16. However, the Bank's decision not to equip EDD cards with EMV chips made *all* EDD cardholders more vulnerable and significantly increased the likelihood that those cardholders would become the victims of having their personal information accessed through skimming. *See infra*, §III.C.

9. Because skimming and counterfeit fraud on the EDD portfolio was already documented in 2019 and highly foreseeable in 2020, it continues to be my opinion that a sophisticated financial institution like the Bank would have known that many EDD cardholders reporting unauthorized PIN-enabled ATM withdrawals in 2020 and 2021 were true victims of counterfeit card fraud (again, fraud that the Bank itself could have prevented simply by issuing EMV chip cards requiring an investment of only [redacted] per card).[4] The Bank's assumption underlying CFF-1—that nearly every cardholder reporting an unauthorized ATM withdrawal was a fraudster filing a false claim—was therefore unfounded. A sophisticated financial institution in the Bank's position should have known and would have known that an automated filter with such a simplistic criterion for disqualifying a claim would likely disqualify many legitimate victims of counterfeit fraud—yet another point that Joseph does not dispute.

III. STATEMENT OF OPINIONS AND BASIS FOR OPINIONS

A. EMV Chips are Extremely Effective at Preventing Card Present Counterfeit Fraud, While Mag-Stripe Only Cards Are Highly Vulnerable to Counterfeit Fraud and Are Thus the Frequent Target of Skimming Attacks.

10. EMV chips are widely recognized for their efficacy at preventing the only kind of fraudulent transaction relevant in this lawsuit: card-present counterfeit fraud at ATMs.

11. The Joseph Report states that "EMV chip cards can also be skimmed, just as magstripe-only cards can," Joseph Rep. ¶32, and that "EMV chips do not prevent cards from being vulnerable to skimming," Joseph Rep. ¶14. Those statements are irrelevant to the issues in this case and to my prior report. EMV technology was not designed to prevent the skimming of mag-stripe data, and I have not suggested otherwise. Rather, as explained in the Cloninger Report, EMV chips were designed to protect against counterfeit card fraud by making stolen data useless for subsequent card-present transactions; and it is widely recognized throughout the

[4] Ex. 27 at -351839-40. *See also* Cloninger Rep. ¶53 n.77.

industry that they are highly effective at doing so. Joseph's focus on the fact that EMV chips do not prevent the skimming of mag-stripe data has little if anything to do with the relevant issue, addressed in my Report, which is that the use of EMV chips prevents the type of card-present transactional *fraud* that skimming attacks are undertaken to facilitate.

12. As I explained in my original report, EMV chip cards, like non-EMV cards, contain magnetic stripes containing cardholder information, such as the cardholder's name and card number. Cloninger Rep. ¶31. Skimming takes place when criminals surreptitiously install a device capable of reading the information on a magnetic stripe on an ATM's card reader and a pinhole camera or PIN pad overlay to capture the cardholders' PIN numbers alongside their card data. *See* Cloninger Rep. ¶¶18-25. After obtaining cardholder data, fraudsters can easily generate counterfeit mag-stripe only cards that, in tandem with the captured PIN, can be used to make cash withdrawals from ATMs or POS terminals. *See id.*

13. EMV technology was not designed to prevent the capture of mag-stripe data – it was designed to disrupt the second stage of the above-described process: the counterfeit fraud itself. Unlike mag-stripe only cards, EMV cards contain an EMV chip, which generates a dynamic code unique to each transaction that is required for a normal transaction to proceed. Cloninger Rep. ¶¶29-31. The EMV chip prevents any *use* of information stolen from an EMV chip card's mag-stripe in two ways. First, an EMV chip is next to impossible to clone, so a counterfeit card with stolen EMV chip card data will not be capable of generating the appropriate dynamic code required for normal transactions. Second, if fraudsters were to attempt to use just the stolen mag-stripe data from an EMV card without the dynamic EMV chip code, the resulting transaction would either be declined or subject to additional security rules specific to fallback transactions. That is because the terminal (POS or ATM) would include a code that informs the issuer that that a chip *should* be present but the magnetic stripe alone was used, and, as a result,

the transaction is flagged as fallback. At that point, the issuer (here, Bank of America) can decide whether to decline or approve the transaction and/or to impose additional security rules. EMV technology thus protects against the creation of functional counterfeit cards, and thereby protects against the use of data captured in a skimming attack to facilitate counterfeit fraud. Cloninger Rep. ¶¶29-33.

14. For similar reasons, "shimming" attacks are also unable to generate a successful clone of an EMV card that can be used to carry out fraudulent ATM withdrawals or other transactions, contrary to Joseph's suggestion. Joseph Rep. ¶¶40, 46, 48, 78. Shimmers are paper-thin devices that are inserted into the chip card reader. Fraud rings place a shimmer inside the chip card reader to record the information transmitted between the chip and the ATM or POS terminal. Shimming devices capture the *one-time* dynamic code (making it fixed and static, not dynamic and ever-changing) and other cardholder data that an EMV chip card transmits to an ATM or POS terminal during that particular transaction. Fraudsters then copy the chip data, including the one-time chip code, onto the magnetic stripe of a counterfeit card. Shimmers do not enable the dynamic-functioning EMV chip itself to be cloned.

15. In 2016, NCR Corporation, one of the largest ATM manufacturers, described shimming in an alert to customers and wrote: "The only way for this attack to be successful is if a [bank card] issuer *neglects to check the CVV* when authorizing a transaction."[5] The alert continued: "All issuers MUST make these basic checks to prevent this category of fraud. Card Shimming *is not a vulnerability with a chip card, nor with an ATM*, and therefore it is not necessary to add protection mechanisms against this form of attack to the ATM."[6]

---

[5] KrebsOnSecurity, *ATM 'Shimmers' Target Chip-Based Cards* (Jan. 27, 2017), https://krebsonsecurity.com/2017/01/atm-shimmers-target-chip-based-cards/ (emphasis added).

[6] *Id.* (emphasis added).

16. In questioning the efficacy of EMV chips in preventing fraud, the Joseph Report principally focuses on *other* types of fraud and, with respect to fraud committed through card-present transactions at chip-reader enabled devices (like most ATMs), her Report focuses on the infrequent exceptions to the general rule that the transaction cannot proceed in the absence of a valid EMV chip card. I explain in detail why the exceptions on which Joseph relies are unable to account for a significant amount of the unauthorized transactions at issue in this case in §III.B, *infra*.

17. Finally, the increase in skimming attacks in 2022 that Joseph discusses does not mean that the use of EMV chips has been unsuccessful at preventing fraud. Joseph Rep. ¶30. Rather, an increase in skimming activity indicates increased targeting of vulnerable mag-stripe only cards. Such a shift was forewarned by industry experts, as discussed in my Cloninger Report and below in §III.C. Cloninger Rep. ¶¶69-73.

18. Nothing in the Joseph Report leads me to change my opinion that EMV chips are highly effective at preventing card-present counterfeit fraud resulting from skimming attacks. Also, much of Joseph's discussion of EMV obfuscates the reality that EMV chip technology, which renders any stolen card information functionally unusable, has significantly reduced card-present counterfeit fraud in every region of the world where it has been introduced, including in the United States. *See* Cloninger Rep. ¶¶34-35, 37. Although EMV does not prevent skimming, it is undisputed that, in the vast majority of cases, it prevents the counterfeit fraud that motivates skimming attacks.

B. Adding EMV Chips to EDD Debit Cards Would Have Prevented the Unauthorized ATM Withdrawals Class Members Experienced.

19. The Joseph Report does not expressly dispute that EMV technology is an effective fraud deterrent, nor could it. Joseph Rep. ¶29. The overwhelming consensus in the payments industry is that EMV technology has been extraordinarily effective in reducing card-

present counterfeit fraud since it was introduced in the 1990s and as its use has become more universal. *See* Cloninger Rep. ¶¶29-45; *see also* Joseph Rep. ¶20 (recognizing the development of EMV in the 1990s and the technology's subsequent "widespread" adoption). Internal Bank documents acknowledge the efficacy of EMV at preventing card-present counterfeit fraud resulting from skimming attacks.[7]

20. Despite clear evidence that EMV technology prevents card-present counterfeit fraud, Joseph opines that "EMV chips would not have prevented many of the card-present transactions that actually involved [redacted]," Joseph Rep. ¶15(b), because [redacted], Joseph Rep. ¶¶15(b), 40. For reasons discussed below, Joseph's statements are grossly exaggerated.

21. The Joseph Report also tries to distract from the established efficacy of EMV at preventing counterfeit fraud by discussing *other* types of fraud that the use of EMV chips would not have prevented, including, for example, card-not-present fraud (principally, online fraud) resulting from data breaches or the random generation of numbers. Joseph Rep. ¶¶31, 42, 59. But those types of fraud are not at issue in this case, and it is therefore irrelevant whether EMV technology would prevent them. By definition, the classes in this case only include EDD debit cardholders who reported an unauthorized, card-present, PIN-enabled ATM withdrawal (sometimes accompanied by additional unauthorized POS transactions, which are also card-

[7] Ex. 25 at -167022 ([redacted]"); Ex. 29 at -12412 ("[redacted]"); Ex. 55 at -163307 ("[redacted]"); Ex. 56 at -172471-72 ("[redacted]"); Ex. 164 at -57505 ([redacted]").

present transactions) – which, in my opinion and as discussed below, an EMV chip almost certainly would have prevented.[8]

1. EMV Chips Would Have Prevented All or Nearly All of the Unauthorized ATM Withdrawals and Other Card-Present Transactions that Class Members Experienced, Because Fallback Transactions Are Limited by Strict Security Rules and Controlled in Frequency.

22. The Joseph Report opines that "EMV chips would not have prevented many of the card-present transactions that actually involved [redacted]" Joseph Rep. ¶15(b). In making these assertions, Joseph relies on a grossly overstated risk of fraud resulting from "fallback transactions," or transactions completed using the mag stripe of an EMV chip card rather than the chip card itself – which Joseph describes as "alternative" transactions. Joseph Rep. ¶24. As I explain below, Joseph ignores that fallback transactions are limited by significant security measures over which the Bank would exercise control, that the Bank did in fact put such controls in place for its non-prepaid consumer debit card portfolio with great success in preventing counterfeit fraud, and, finally, that fallback transactions comprise a small number of overall transactions.

23. When an EMV chip cardholder attempts to make a transaction at a chip-enabled terminal by swiping the mag-stripe rather than inserting the chip, the data in the mag-stripe from the EMV card will indicate to the ATM or POS terminal that a chip should be present, and the

[8] Despite Joseph's extensive discussion of first-party and benefits fraud, neither my previous nor this Report addresses such fraud. Joseph Dec. ¶¶15(a), 58, 61-66. My understanding is the class definition excludes any individual who the Bank determines [redacted]" Ex. 74 at -102557.

ATM or POS terminal will detect that a mag-stripe (as opposed to the chip) has been presented and will request that the chip be used. The same thing happens when a fraudster attempts to make a transaction at a chip-enabled terminal using a cloned mag-stripe-only version of an EMV chip card. Because the counterfeit mag stripe contains a service code that indicates the card has an EMV chip, the ATM or POS terminal will recognize that a mag-stripe on a chip card has been presented and will request that the chip be used. If no chip (or a damaged chip, or a mismatched chip with the wrong code, as Joseph theorizes) is then presented, the ATM or POS terminal can decline the transaction.

24. The only exception is a "fallback" transaction, which occurs when, instead of declining the transaction, the ATM or POS terminal allows the cardholder to "fallback" and use the mag-stripe of a detected chip card to make the transaction. Before allowing a fallback transaction, the ATM or POS terminal will typically send a code to the card issuer notifying the issuer that a mag-stripe transaction has been requested with a chip card because if they do not, then liability for any fraudulent fallback transactions falls on the merchant or ATM operator.[9] The issuer can then require additional security checks, decline the transaction, or approve the transaction with or without withdrawal limits. If the merchant or ATM operator provides this fallback notice code to the issuer and the issuer authorizes the fallback transaction, then liability for the fallback transaction, if it proves to be fraudulent, falls on the issuer.

25. Here, Joseph completely ignores that Bank of America was the issuer of all EDD debit cards and thus, control over the possibility of fallback fraud would have rested principally with the Bank.

---

[9] *EMV Implementation Guidance: Fallback Transactions*, US Payments Forum 1 (2016), https://www.uspaymentsforum.org/wp-content/uploads/2017/03/Fallback-Transaction-Guidance-FINAL-Dec-2016.pdf; Ann Davidson, *Fraud & Fallback: What You Need to Know About Skimming Attacks*, Credit Union Times (Sept. 16, 2024), https://www.cutimes.com/2024/09/16/fraud-fallback-what-you-need-to-know-about-skimming-attacks/?slreturn=20241116-43702.

26. Joseph also ignores that the Bank [redacted].[10]

27. [redacted], one Bank employee explained:

- [redacted][11]

28. The Bank acknowledged [redacted].[12]

29. By 2021, one Bank employee described [redacted].[13]

30. Thus, in 2020, had the Bank equipped its EDD debit cards with EMV chips and [redacted], any criminal who attempted to use a counterfeit card with a deliberately broken chip at an ATM would have been [redacted]

[10] *See, e.g.*, Ex. 32 at -228914.

[11] *Id.*

[12] Ex. 164 at -57505.

[13] Ex. 165 at -431012.

[redacted].[14] [redacted]

[redacted].

31. Joseph provides no explanation why the Bank would not have [redacted] I am aware of no reason why [redacted].

32. The Bank's [redacted] The Bank experienced [redacted][15] Were fallback transactions as significant a weakness in EMV protection against fraud as the Joseph Report suggests, one would expect [redacted] significantly undermines Joseph's argument that EMV would not have similarly protected EDD cardholders in 2020.

[14] There are three types of "CVV numbers" relevant to a payment transaction. The CVV2 that is printed on the back of the card is unrelated to the CVV number written on the mag stripe (described in Cloninger Rep. ¶17) and the iCVV (frequently called dynamic CVV) that can be generated only by an EMV chip. When the Bank requests the cardholder to enter their CVV2 number, it is the number that is printed on the back of the card, as the cardholder cannot see either of the other two. This step provides assurance that the card is in the cardholder's possession. *See Mitigating Fraud Risk Through Card Data Verification*, Visa Business News (Oct. 8, 2015), https://www.cba-ok.org/wp-content/uploads/2016/09/VBN-Mitigating-Fraud-Risk-Through-Card-Data-Verification-002.pdf.

[15] Ex. 34 at -297295 ("[redacted]"). My understanding is that "[redacted]" refers to the Bank's non-prepaid consumer debit cards, all of which had EMV chips as of 2014. Ex. 23.

33. Joseph's discussion of the various scenarios that lead to fallback transactions might suggest that such transactions are common, but that is not the case. Fallback transactions had been high during the initial years of EMV deployment, largely due to problems with implementation. As a result, 75% of card issuers rolled out new policies to "decline authorization of high-dollar fallback purchases," while others focused on merchants with abnormally high fallback rates and other methods to control the use of fallbacks.[16] However, by 2017, fallback transactions represented less than 2% of overall purchase authorizations and fraud related to those transactions was falling rapidly as a result of industry mitigation efforts, including the use of fallback rules.[17] In addition to fallback rules, other industry mitigation efforts include imposing transaction fees to penalize frequent fallback transactions. If fallback transactions at a given ATM exceed 2.5% for Visa or 3.0% for Mastercard, the networks impose penalty fees.[18] The penalty fees imposed by the networks provide merchants and ATM operators with incentives to ensure that their equipment is properly functioning and to investigate any increases in fallback rates.

34. Thus, in 2018, fraud data showed that fallback fraud represented only 11.5% of counterfeit fraud, down from more than 20% in 2017, and only 3.2% of overall credit card fraud, down from 4.5% in 2017, declines of 45% and 30% year over year.[19] There is no reason not to

---

[16] *Credit Card "Fallback" Fraud Declines Significantly as Banks Implement New Policies*, Auriemma Roundtables: Industry Analysis (Nov. 7, 2018), https://roundtables.us/credit-card-fallback-fraud-declines-significantly-as-banks-implement-new-policies/.

[17] *Id.*; Ann Davidson, *Fraud & Fallback: What You Need to Know About Skimming Attacks*, Credit Union Times (Sept. 16, 2024), https://www.cutimes.com/2024/09/16/fraud-fallback-what-you-need-to-know-about-skimming-attacks/?slreturn=20241116-43702 ("Both chip cards and readers undergo rigorous testing and certification, making fallback incidents exceptionally rare.").

[18] *Id.*

[19] *Credit Card "Fallback" Fraud Declines Significantly as Banks Implement New Policies*, Auriemma Roundtables: Industry Analysis (Nov. 7, 2018), https://roundtables.us/credit-card-fallback-fraud-declines-significantly-as-banks-implement-new-policies/.

believe that fraud rates continued at or below these rates over the subsequent two years and beyond.

35. The Joseph Report thus grossly overstates the likelihood of fraud through fallback transactions and ignores that the Bank's own rules significantly limited such fraud *in 2020 and 2021* on its non-prepaid consumer debit card portfolio. It thus continues to be my opinion that including EMV chips on the Bank's EDD debit cards would have been highly effective in preventing the vast majority of unauthorized transactions attributable to card-present counterfeit fraud that class members experienced.

2. *Joseph Does Not Present Any Evidence that Non-Counterfeit Fraud Affected More than a De Minimis Number of Class Members.*

36. Joseph contends that the use of EMV chip cards would not have prevented unauthorized transactions resulting from lost or stolen cards or from a cardholder's mistaken assertion that a transaction was not authorized. However, Joseph does not cite any evidence suggesting that these were circumstances that affected any substantial number of class members. As I explain below, neither of these scenarios (lost/stolen cards or mistake/family use), in my professional experience, likely account for more than a small percentage of total unauthorized transaction claims.

37. First, fraud resulting from a lost or stolen card generally comprises a small percentage of overall reports of fraudulent transactions. A 2024 survey conducted by Security.org found that "only 7% of fraudulent charges involved stolen or lost credit cards," meaning the remaining 93% of fraudulent charges involved cards still in the owner's possession.[20] Because all class members in this case reported PIN-enabled transactions, in Joseph's hypothetical, fraud resulting from lost or stolen cards would also require the cardholder to have [redacted]. Joseph Rep. ¶¶80-83. Joseph provides no evidence for why

[20] Brett Cruz, *52 Million Americans Experienced Credit Card Fraud Last Year: 2024 Credit Card Fraud Report and Statistics*, Security.org (Jul. 26, 2024), https://www.security.org/digital-safety/credit-card-fraud-report/.

such a unique factual scenario leading to fraud would comprise any significant portion of the unauthorized transactions class members experienced.

38. A claim of an unauthorized transaction resulting from a cardholder's honest mistake (not recognizing the transaction) or from a family member's authorized use of the card is also highly unlikely to explain any significant number of the unauthorized transactions class members reported.

39. The lone source that Joseph cites for this possibility is a Lending Tree survey about card sharing between parents and children, but Joseph offers no rationale for assuming that the survey results are applicable to this particular category of EDD debit cardholders. Joseph Rep. ¶67 n.31. According to that Lending Tree survey, instances of children spending without permission include "in-app or in-game purchases (28%), ordering food delivery (16%)… making purchases through voice-activated speakers (15%)," buying clothes (14%), buying "toys or games" (13%), or buying "something else" (1%).[21] The survey does not discuss children using their parents' cards to make unauthorized ATM withdrawals.

40. In conclusion, it continues to be my opinion that EMV chips would have "prevented virtually all card-present counterfeit fraud (including unauthorized ATM withdrawals) for the Bank's EDD debit cardholders at chip-enabled ATMs and POS terminals." Cloninger Rep. ¶14(h). Nothing in the Joseph Report changes my opinion that EMV is the right tool to have prevented the card-present ATM fraud that is at issue in this case.

3. Individual inquiries are not necessary to determine if EMV would have prevented these unauthorized transactions.

41. The Joseph Report opines that determining whether a particular unauthorized transaction could have been prevented by an EMV chip card would be a highly fact-dependent inquiry into the circumstances of the transaction. Joseph Rep. ¶¶44-50. I disagree.

[21] Dawn Papandrea, *46% of Parents Say Their Child Used Their Credit or Debit Card Without Permission, Racking Up $500+*, Lending Tree (Mar. 1, 2022), https://www.lendingtree.com/credit-cards/study/kids-and-credit-cards-survey/.

42. For all the reasons discussed above, the threshold factual scenario necessary to determine whether EMV would have prevented a transaction is simply whether it was card-present counterfeit fraud. Once that determination is made, no additional inquiry is needed as to the ability of EMV to have prevented the resulting fraud.

43. As described in §III.B.2., no other type of fraud (e.g. lost/stolen card) could account for a significant, or even more than de minimis, number of the card-present, PIN-enabled ATM transactions that class members reported.

44. Nonetheless, my understanding is that the Bank has in its records system details about each claim, including [redacted].[22] No intensive fact inquiry would be needed, then, to distinguish the few class members whose transactions may have resulted from [redacted] – they would have been recorded as [redacted]. The Bank also possesses data collected with every claim as to whether [redacted].[23] Again, the Bank could easily disaggregate those individuals from the people who [redacted].

/ / /

[22] *See* Ex. 166 at -205593 ("[redacted]"); *see, e.g.*, Ex. 14 (Daniels Tr.) 79:5-80:4 ([redacted] …"); Ex. 167 at -001199 ("[redacted]").

[23] *Id.*

4. Joseph's Opinions that EMV Chips Would Not Prevent Other Types of Fraud Are Irrelevant.

45. The Joseph Report devotes considerable space to addressing irrelevant issues, for example, by asserting that EMV chips would not have prevented unauthorized card-not-present transactions, which are primarily online transactions. Card-not-present transactions are not relevant to this case. By definition, every class member reported an unauthorized ATM withdrawal, which is necessarily a card-present transaction.

46. Joseph's assertion that EMV chips might not have prevented certain other types of fraud that might have affected class members, such as [redacted], is also irrelevant. Joseph Rep. ¶¶31, 42, 51(b), 87. I do not contend in the Cloninger Report that EMV chips would prevent data breaches or phishing attacks, which could enable fraudsters to create counterfeit cards using the stolen information. My principal opinion has consistently been that, for the reasons discussed above, EMV chips are effective at protecting against any unauthorized card-present transactions, particularly at an ATM machine, that a fraudster may attempt with a counterfeit card created using the information stolen from a data breach or phishing attack. If the Bank had issued EDD cards with EMV, either the transaction would be declined because no chip was present or the Bank's fallback rules would stop or significantly limit the transaction. Again, because all class members here reported an unauthorized ATM withdrawal, which is necessarily a card-present transaction, the inclusion of an EMV chip in EDD debit cards would have prevented all or nearly all of those ATM withdrawals.

C. The Bank's Failure to Include Industry-Standard EMV Chips in EDD Debit Cards in 2020 Caused Those Cards to Be Susceptible to and Targeted for Skimming.

47. As explained in my previous report, EMV technology had by 2019 already become the well-established industry standard for card security in the United States—a point that Joseph does not dispute. Cloninger Rep. ¶¶36-45.

48. By early 2020, the Bank understood that counterfeit fraud was a problem for its EDD portfolio and that EMV offered a solution, at minimal cost to the Bank.[24] For an incremental cost of only $[redacted] per card, the Bank predicted [redacted].[25] In one Bank official's own words, despite [redacted], "[redacted]." Cloninger Rep. ¶¶48-56.

49. Nevertheless, the Bank chose not to include EMV chips in EDD debit cards in 2020. I continue to adhere to my prior opinion that the Bank's decision *not* to equip EDD cards with EMV chips in 2020 was highly irregular and resulted in the issuance of highly vulnerable cards with below-industry-standard security. Based on my 35 years of experience in the payments industry, it is my view that the Bank's decision was particularly unreasonable and irresponsible given the heightened vulnerability of this cardholder population and the Bank's contractual promises to EDD to provide the "highest level of security and fraud safeguards."[26]

50. As already explained above, the lack of an EMV chip in a mag-stripe only card renders that card susceptible to skimming and to counterfeit card fraud. The Bank's failure to issue industry-standard EMV chip cards to EDD cardholders subjected all EMV Chip class members to an unnecessary and heightened risk of unauthorized access to and disclosure of information on their EDD debit cards and in their EDD debit cards accounts—including from skimming and from any subsequent uses of their skimmed information.

---

[24] Ex. 25 at -167022 ([redacted]"); Ex. 29 at -124142 ([redacted]"); Ex. 27 at -351839-40; Ex. 16 (Martin Tr.) 82:8-83:13.

[25] Ex. 27 at -351839-40; Ex. 16 (Martin Tr.) 82:8-83:13.

[26] Cloninger Rep. ¶46 (quoting Ex. 22 at 253-54).

51. The Joseph Report also opines that, "In order to determine whether an EMV chip would have prevented access to or compromise of information on an EDD prepaid debit card, one would have to look at the circumstances surrounding the access or compromise. Joseph Rep. ¶16. For several reasons, I disagree.

52. First, the Bank's decision not to equip EDD cards with EMV chips made *all* EDD cardholders more vulnerable and significantly increased the likelihood that those cardholders would become the victims of having their personal information accessed through skimming. That increased vulnerability and susceptibility to unauthorized access of their personal information does not depend on those cardholders' individual circumstances. Rather, that susceptibility applies to all class members because they were regularly receiving substantial amounts of money on mag-stripe only debit cards without EMV chip protection. Joseph does not take issue with the well-documented fact that fraud rings use skimming technology to specifically target mag-stripe only cards, particularly where the value loads on those cards are larger (i.e., a combination of increased vulnerability and higher pay-off per skimmed card). The Bank's decision not to include EMV chips in the EDD debit cards portfolio, which grew rapidly in value load during the pandemic, foreseeably led to increased skimming attacks targeting EDD cards in California, a predictable increase that the Bank's own documents demonstrate the Bank was aware of. Accordingly, the issuance of mag-stripe only EDD cards put each EDD cardholder at much higher risk for unauthorized access and use and disclosure of personal information.

53. Joseph speculates that EMV chip cards are just as vulnerable as mag-stripe-only cards to being skimmed and then cloned for purposes of making counterfeit transactions. As explained above, this is untrue. There is little incentive for fraudsters to attempt to make fraudulent card-present transactions using counterfeit versions of EMV chip cards, because those fraudulent transaction attempts will fail in most instances. There is even less reason for fraudsters

to attempt fraudulent transactions with counterfeit versions of EMV chip cards, given that mag-stripe only cards, like the EDD debit cards at issue here, are far easier and far more profitable targets. As the Joseph Report acknowledges, "[redacted]" Joseph Rep. ¶72. By 2020, vulnerable mag-stripe only cards like the EDD debit cards that the Bank issued to class members were that "[redacted]." Had the Bank issued EMV chip cards to EDD cardholders, criminals would have had little incentive to target them with skimming attacks. Thus, it was highly foreseeable that the lack of EMV chips on EDD debit cards would lead to increased counterfeit fraud specifically targeting EDD cardholders during the pandemic. *See* Cloninger Rep. ¶¶69-85.

54. This foreseeable outcome of the Bank's decision not to issue EMV chip cards to EDD cardholders is exactly what happened. The Bank had observed that by 2019, counterfeit fraud was already a significant problem and rising on the EDD portfolio.[27] In 2020 and 2021, the Bank observed an "[redacted] specifically.[28] One Bank employee observed that "[redacted]."[29] Another noted that "[redacted]."[30] The Bank's decision not to issue EMV chip cards thus foreseeably led to an increase in skimming attacks on vulnerable EDD cards, particularly as their load value increased during the pandemic.

---

[27] *See* Cloninger Rep. ¶¶78-84; *see also* Ex. 25 at -167022 ("[redacted])").

[28] Ex. 168 at -166345 ("[redacted]").

[29] Ex. 26 at -370154.

[30] Cloninger Rep. ¶¶78-80 (quoting Ex. 34 at -297295).

55. Second, for every class member who experienced an unauthorized ATM withdrawal while their EDD debit card was still in their possession, the most likely explanation is that the unauthorized transaction was committed using a counterfeit card created as a result of skimming. Joseph asserts that "skimming or shimming would not capture the PIN." Joseph Rep. ¶77. This assertion completely ignores the widely known fact, explained in the Cloninger Report and acknowledged in the Bank's own documents, that skimmers are typically used in conjunction with pinhole cameras or a PIN pad overlay that captures the cardholder's PIN to be used in conjunction with the skimmed magstripe data. *See* Cloninger Rep. ¶¶18-25.[31]

IV. CONCLUSION

56. By issuing mag-stripe only cards to EDD debit cardholders, the Bank increased the likelihood of unauthorized access, theft, and disclosure of their personal information in two ways: first, it issued EDD beneficiaries cards that were extremely susceptible to unauthorized disclosure of personal information through skimming and counterfeit attacks, and second, the issuance increased the likelihood those cards would in fact be compromised by skimming attacks and counterfeit card fraud. From a card-security perspective, the Bank left cardholders entirely empty handed while slapping a target on their backs.

57. The Joseph Report's conclusion that EMV would not have prevented many of the unauthorized transactions that class members experienced is unsupported by evidence and is directly contradicted by the Bank's own internal documents, which recognize that the use of EMV chips on its *non-prepaid consumer debit cards* effectively prevented counterfeit fraud even when they were skimmed by the same skimmers that resulted in counterfeit fraud being perpetrated against EDD debit cardholders. Joseph's statement that EMV chips can also be

[31] Ex. 33 at -455617 ("[redacted]") (emphasis added); Ex. 168 at -166345 ("[redacted].").

counterfeited grossly overstates that risk. It is widely accepted throughout the payments industry that EMV chips are extremely effective at preventing card-present counterfeit fraud, particularly unauthorized ATM withdrawals.

58. Joseph's opinion that individualized inquiries would be necessary to determine whether EMV chips would have prevented the disputed unauthorized transactions ignores that all class members reported the same type of unauthorized transaction: an unauthorized ATM withdrawal. Because an unauthorized ATM withdrawal is necessarily a card-present transaction with a PIN, the most likely explanation is that class members were the victims of skimming, as skimming operations (unlike data breaches) typically enable the fraudster to capture the PIN in addition to the data contained on the mag-stripe. Moreover, as the Bank's own documents recognize, the Bank's issuance of mag-stripe only EDD debit cards during the pandemic with growing value loads made those cards an attractive target and foreseeably led to a rise in skimming attacks specifically targeted at mag-stripe only EDD debit cards. Skimming is thus the most likely explanation for the unauthorized ATM withdrawals and other unauthorized card-present transactions that class members experienced.

59. For all these reasons, nothing in the Joseph Report changes my opinion that the Bank could not have reasonably assumed that *all* or even a majority of EDD cardholders reporting unauthorized PIN-enabled, card-present transactions were committing first-party fraud. To the contrary, it remains my opinion that any financial institution in the Bank's position would have known that many EDD cardholders reporting unauthorized ATM withdrawals were true victims of skimming and counterfeit fraud.

* * * * * *

Dated: November 21, 2024

Jane E. Cloninger

Appendix A: List of Additional Materials Considered

Date	Document Type	Title/Description	Bates Range
2/6/2024	Transcript	Transcript of Rule 30(b)(6) Deposition of Shane Daniels	
2/29/2024	Transcript	Transcript of Rule 30(b)(6) Deposition of William ("Matt") Martin	
2/16/2024	Transcript	Transcript of Rule 30(b)(6) Deposition of Michael Letson	
8/29/2024	Report	Expert Report of Jane Cloninger in Support of Plaintiffs' Motion for Class Certification (Ex. 2 to the Declaration of Connie Chan in support of Plaintiffs' Motion for Class Certification) ("Cloninger Rep.")	
10/24/2024	Report	Declaration of Pamela Joseph (DX 4 to the Declaration of Laura Brys in support of Defendant's Opposition to Plaintiffs' Motion for Class Certification) ("Joseph Rep.")	
10/8/2015	Article	Mitigating Fraud Risk Through Card Data Verification	
3/1/2022	Article	"46% of Parents Say Their Child Used Their Credit or Debit Card Without Permission, Racking Up $500+"	
7/26/2024	Article	"52 Million Americans Experienced Credit Card Fraud Last Year"	
3/23/2021	Article	"ATM fallback fees, and how to prevent them"	
9/16/2024	Article	"Fraud & Fallback: What You Need to Know About Skimming Attacks"	
11/7/2018	Article	"Credit Card "Fallback" Fraud Declines Significantly as Banks Implement New Policies"	
Rep. 2016	Report	"EMV Implementation Guidance: Fallback Transactions"	
1/27/2017	Article	"ATM 'Shimmers' Target Chip-Based Cards"	
7/10/2015	Document	Excerpts of BANA's Response to State of California Electronic Benefits Payments RFP Vol I & II	
12/29/2020	Email	[redacted]	BANA_EDD_MDL - 090640-90647

1/10/2020	Email	[redacted]	BANA_EDD_MDL - 351839-351840
3/13/2020	Email		BANA_EDD_MDL - 167019-167024
2/21/2020	Email		BANA_EDD_MDL - 124142
11/2/2020	Email		BANA_EDD_MDL - 163307-163308
7/10/2020	Email		BANA_EDD_MDL - 172469-172473
10/12/2022	Document		BANA_EDD_MDL - 102554-102577
4/24/2020	Email		BANA_EDD_MDL - 228914-228915
4/23/2021	Email		BANA_EDD_MDL - 297295
1/10/2020	Email		BANA_EDD_MDL - 351839-351840
1/28/2020	Email		BANA_EDD_MDL - 370150-370155
8/18/2020	Email		BANA_EDD_MDL - 455617-455619
10/30/2020	Email		BANA_EDD_MDL-00057504-06
2/9/2021	Email		BANA_EDD_MDL-00431011-14
9/14/2020	Email		BANA_EDD_MDL-00205593-97
	Document		BANA_EDD_MDL-00001199
	Presentation		BANA_EDD_MDL-00166345