

EXHIBIT 4

**FILED
PROVISIONALLY
UNDER SEAL WITH
REDACTIONS
PURSUANT TO
STIPULATED
PROTECTIVE ORDER**

CONFIDENTIAL

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA
SAN DIEGO DIVISION**

IN RE: BANK OF AMERICA
CALIFORNIA UNEMPLOYMENT
BENEFITS LITIGATION

Case No. 3:21-md-02992-GPC-MSB

DECLARATION OF PAMELA JOSEPH

October 24, 2024

FILED PROVISIONALLY UNDER SEAL
PURSUANT TO STIPULATED PROTECTIVE ORDER

CONFIDENTIAL

Table of Contents

I. Qualifications	3
II. Assignment.....	4
III. Summary of Opinions	5
IV. Background.....	6
V. Chip cards do not prevent skimming or other forms of information compromise.....	9
A. Card fraud continues to increase in the U.S. despite the adoption of EMV chips on many cards	9
B. EMV chips do not prevent cards from being skimmed or card information from otherwise being compromised.	10
C. The determination of whether an EMV chip would have prevented skimming or other information compromise requires examination of each particular incident of compromise	13
VI. Adding chips to EDD prepaid debit cards issued by the Bank would not have prevented many of the unauthorized transactions reported to the Bank in 2020	15
A. The shifting of liability for fraud does not eliminate fraud	17
B. EMV chip cards do not prevent all fraud	18
C. Chips would not have prevented the allegedly unauthorized transactions that involved fraud or mistake by the cardholder	19
D. Chips would not have prevented all fraudulent ATM withdrawals reported to the Bank that were actually unauthorized	22
E. EMV chips would not have prevented all fraudulent point-of-sale transactions	27
F. The determination of whether an EMV chip would have prevented a particular unauthorized transaction requires examination of each transaction.....	28
VII. Conclusion	29

CONFIDENTIAL

I. Qualifications

1. I have over 30 years of experience in the electronic payments industry. I have held executive positions as the CEO, COO and President of several large U.S. payment companies and have overseen business lines that included consumer credit and debit card issuing, corporate card issuing, prepaid and fleet card programs, as well as state Electronic Benefits Transfer (“EBT”) programs. I have also overseen large global merchant acquiring businesses.

2. Currently, I am an Operating Partner with Advent International and CEO for Xplor Technologies, a global vertical SAAS provider in Everyday Life Verticals. Xplor Technologies also operates a proprietary global payment processing platform.

3. Prior to joining Advent, I served as President and Chief Operating Officer of Total System Services, Inc (“TSYS”). At TSYS, I was responsible for overseeing all business lines including providing issuing services for 55% of the bank cards issued in the U.S. TSYS also owned the second largest prepaid card business in the U.S. I was responsible for building out a global product division, building out the merchant acquiring business, and developing programs utilizing artificial intelligence to better combat card fraud.

4. Prior to joining TSYS, I served as a Vice Chair of U.S. Bancorp’s payment services division, representing over \$5 billion in revenue for the bank. I had responsibility for all electronic payment product lines including consumer credit and debit cards, corporate and small business cards, and prepaid cards. Additionally, I oversaw EBT programs for many states in the U.S. I was also chair of Elavon, a global merchant acquiring business. I joined U.S. Bancorp in 2001 through its acquisition of Elavon.

5. Before joining Elavon, I served with Visa International as director of all new market development and acceptance.

CONFIDENTIAL

6. I currently serve as a public company board director for Paychex and Adyen, and serve as chair of the board of Transunion.

7. My curriculum vitae is attached as Appendix A.

8. I am being compensated at a rate of \$600 per hour.

9. In conducting my work on this matter, I have been assisted by individuals at Ankura Consulting Group, LLC (“Ankura”),¹ who worked at my direction and under my supervision. All opinions expressed herein are my own.

10. I have not provided expert testimony in the past four years, and I have not authored any publications in the past ten years.

11. In preparing this declaration, I personally considered various documents produced in this litigation and other materials, which are identified in Appendix B.

II. Assignment

12. I have been retained by Goodwin Procter LLP, on behalf of Bank of America, N.A. (“Bank of America” or the “Bank”) in connection with the above matter. I was asked to provide background on magnetic stripe (“magstripe”) technology as well as Europay, Mastercard, and Visa (“EMV”) chip class technology in prepaid debit cards. I was also asked to review and respond to certain opinions expressed in the Expert Report of Jane Cloninger in Plaintiffs’ Motion in Support of Class Certification dated August 29, 2024 (PX 2, “Cloninger Report”). Finally, I was asked to review and respond to certain opinions expressed in the Expert Class Certification Report by Greg J. Regan, CPA/CFF, CFE dated August 29, 2024 (PX 4, “Regan Report”) as they relate to the

¹ Ankura is a professional services and consulting firm that provides dispute-related, investigative, financial, and operational consulting services to various types of organizations.

CONFIDENTIAL

purported EMV chip class. In particular, I was asked to provide my opinion on the following topics:

- a. Whether EMV chips would have prevented card skimming, card shimming, or other unauthorized access to cardholder information stored on a prepaid debit card.
- b. Whether the addition of EMV chips to the Employment Development Department (“EDD”) prepaid debit cards issued by the Bank would have prevented the alleged unauthorized transactions that were reported to the Bank in 2020.

13. This report does not respond to all of the opinions in the Cloninger Report or the Regan Report. It only responds to those specific opinions or assumptions that counsel has asked me to respond to for purposes of opposing Plaintiffs’ Motion for Class Certification. I reserve the right to respond to additional opinions or assumptions in the Cloninger Report and/or the Regan Report if asked to do so by counsel in the future.

III. Summary of Opinions

14. EMV chips do not prevent cards from being vulnerable to skimming, shimming, or other forms of information compromise.

15. The 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.

- a. EMV chips would not have prevented any of the transactions that did not actually constitute third-party fraud, such as where the cardholder committed first-party fraud or otherwise bore culpability / responsibility for the transaction (*e.g.*, benefits fraud or false or mistaken reports of unauthorized transactions).

CONFIDENTIAL

- b. EMV chips would not have prevented many of the card-present transactions that actually involved [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

- c. EMV chips would not have prevented any [REDACTED]
[REDACTED]. Indeed, Ms. Cloninger cabins her opinion by focusing specifically on card-present fraud, opining that “[t]he addition of EMV chips to the Bank’s EDD debit cards would have prevented virtually all *card-present* counterfeit fraud.”² (emphasis added).

16. 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. Likewise, 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.

IV. Background

17. Magstripe technology was introduced as a means of storing information on plastic cards by IBM in the early 1960s.³ Within the banking and credit card industry, the technology

² Expert Class Certification Report of Jane Cloninger, August 29, 2024, Motion for Class Certification, (PX 2, “Cloninger Report”), ¶ 47.

³ “The magnetic stripe,” IBM, <https://www.ibm.com/history/magnetic-stripe> (Last visited October 18, 2024).

became the most widespread mechanism for authorizing bank and credit card transactions and verifying identities over the course of the 1970s through the 1990s.⁴ As noted by IBM, “Only 16% of US families held a bank card in 1970, while more than two-thirds did in 1998.”⁵

18. Magstripe cards have a magnetic stripe on the back of the card that is made of iron particles in plastic film and contains embedded data. When the card is swiped through the slot on an electronic reader such as a sales terminal in a retail store, the reader decodes the embedded data on the stripe and either approves or rejects the card for payment.

19. The magstripe on a bank debit card contains three horizontally stacked tracks, each of which stretch across the full width of the card and occupy a portion of the magstripe. Each track is capable of holding a different type and amount of data.

20. EMV chip card technology was developed in the 1990s but its usage became more widespread for certain card products (primarily credit cards and consumer debit cards) in the United States in the 2010s. EMV stands for “Europay, Mastercard and Visa,” the three companies that jointly helped develop the EMV chip card standards in the 1990s. EMV chips create a single use code when they are inserted into an EMV card reader to process a payment.⁶ The use of EMV chips increased further when the card network liability rules changed in 2015, allowing issuers of cards with chips to shift the responsibility for fraudulent transactions to any merchants that did not require the chip to be used for payment.

21. However, cards with EMV chips still continued to have magnetic stripes. While Mastercard has announced that it would start issuing cards without magnetic stripes in 2024 in

⁴ *Id.*

⁵ *Id.*

⁶ “What is an EMV chip and how does it store your data?” Chase, <https://www.chase.com/personal/credit-cards/education/basics/what-is-emv-chip-how-it-stores-your-data> (Last visited on October 18, 2024).

regions such as Europe and in 2027 in the United States,⁷ cards in the U.S. with EMV chips in 2020 and 2021 still had a magnetic stripe in addition to a chip (and indeed were required to).

22. Not all businesses in the U.S. offer chip readers; chip readers are not required.

23. Merchants with chip readers also typically offer a card reader that will read magstripes as well. This is because not all cards have EMV chips. This was particularly the case in 2020-2021. EMVCo, a consortium that develops and publishes EMV payment technology specifications and develops related testing processes, reported that 63.8% of cards issued in 2020 had EMV chips.⁸

24. For cards with both EMV chips and magstripes, the magstripe presents an alternative means of completing a transaction if a chip reader is out of service or is not functioning properly. The magstripe can be used if a chip reader is not available at the time the card is used, or is broken, or the merchant does not require a chip.

25. Additionally, chips on cards can be scratched or damaged (*e.g.*, through excessive heat/water) or become dirty and become unreadable. In these instances, the magstripe on the cards is often used for payment, even if a functioning chip reader is available. Indeed, in my experience, it is a common practice for fraudsters to place a cloned magstripe on a card that has a real EMV chip but one that does not match the magstripe, and then damage the chip (for example by placing it over a flame) so that the chip reader registers the card as having a chip, but one that is not functioning, such that payment can be processed using the cloned magstripe.

26. Merchants with chip readers can decide whether to require a chip for payment. Some merchants may opt to let the customer decide (the “either or” approach); some may opt to

⁷ “Swiping left on magnetic stripes”, MasterCard, August 21, 2021, <https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/> (Last visited on October 23, 2024).

⁸ EMVCo 2020 Annual Report, <https://www.emvco.com/wp-content/uploads/2022/09/EMVCo-Annual-Report-2020-1.pdf>.

CONFIDENTIAL

let the customer use a magstripe if the chip or chip reader are not functioning (the “chip first” approach); and others may opt to require chip payments for all cards with EMV chips no matter the circumstances (the “chip only” approach).

27. Further, when a card is used in a card-not-present transaction, card information (card number, cardholder name, expiration date, card verification value or cvv) is entered into a form on a website or mobile application, or is provided to a merchant over the phone. Neither the EMV chip nor the magstripe is used for payment in these instances.

28. Importantly, while EMV chip cards have proven to be successful in mitigating some types of fraud risk, they have by no means eliminated fraud risk. For example, as discussed below, they do not prevent skimming or other forms of information compromise. Also as discussed below, adding chips to prepaid debit cards (such as EDD prepaid debit cards) would by no means prevent all unauthorized transactions, and the effect of an EMV chip would have to be assessed on a case-by-case basis.

V. Chip cards do not prevent skimming or other forms of information compromise

A. Card fraud continues to increase in the U.S. despite the adoption of EMV chips on many cards

29. While EMV chip cards are generally recognized as an additional fraud deterrent in the U.S., Canada, and Europe, they do not fully prevent card information from becoming compromised. Indeed, card fraud has continued to increase, notwithstanding the presence of EMV chips on cards.

30. A December 2020 Nilson Report, which is a periodical specific to the card industry, quantified annual global card-fraud losses at \$23.97 billion in 2017, which then increased 20

CONFIDENTIAL

percent to \$28.65 billion by 2019.⁹ And in the first half of 2022, there was a year-over-year increase of 501 percent in the number of compromised cards detected, indicating that “skimming” was on the rise—even in 2022, following broad adoption of EMV-enabled debit and credit cards.¹⁰

31. The presence of an EMV chip on a card does not eliminate fraud, as reflected in the continued growth in card fraud. Based on my 35 years of experience in the card and payments industry, some of the trends and tactics that can drive the increase in fraud include:

- a. Fraud generated with card numbers stolen in pre-pandemic data breaches.
- b. Phishing attacks, including emails and phone calls, which attempt to trick customers into handing over their card credentials.
- c. The generation of random numbers until a legitimate account is stumbled upon.

B. EMV chips do not prevent cards from being skimmed or card information from otherwise being compromised.

32. Notably, EMV chip cards can also be skimmed, just as magstripe-only cards can, because [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

33. There are multiple scenarios in which an EMV chip card can be skimmed.

34. [REDACTED]

[REDACTED]

⁹ Nilson Report, Issue 1187, December 2020, Page 1.

¹⁰ FICO Blog, August 16, 2022. <https://www.fico.com/blogs/us-card-skimming-fraud-grows-700-first-half-2022> (Last visited October 18, 2024).

CONFIDENTIAL

[REDACTED]

[REDACTED].

35.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

36.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

37. The Cloninger Report describes the skimming process and includes several images of skimmers.¹¹ What the Cloninger Report fails to note, however, is that [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

38. In fact, the materials in this case support the conclusion that not only was it possible to skim chip cards but that such skimming of chip cards actually occurred. As an example, [REDACTED]

[REDACTED]

¹¹ Cloninger Report, ¶¶ 20-25.

CONFIDENTIAL

[REDACTED].¹² [REDACTED]
[REDACTED].¹³ As the Cloninger Report notes, other Bank of America-issued debit cards had EMV chips by this time.¹⁴ Therefore, this document confirms that skimming continued to occur even for cards with EMV chips.

39. EMV chips also do not prevent other forms of information compromise.

40. Beyond skimmers, there are also “shimmers,” which are thin devices that can similarly be inserted into a POS terminal, an ATM, or a gas pump and which target the EMV chip directly—allowing a fraudster to capture data from the chip. The shimmering device is [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED].

[REDACTED]. The Cloninger Report does not consider the existence of shimmers and their ability to compromise information from a chip card.¹⁶

41. Further, EMV chips do not prevent a PIN compromise or have any impact on a PIN compromise at all. Magnetic stripes do not typically contain PIN information;¹⁷ thus, when a magnetic stripe is skimmed, the PIN information is not compromised.

¹² Declaration of Laura Brys in Support of Defendant’s Opposition to Plaintiffs’ Motion for Class Certification, Ex. (“DX”) 41, [REDACTED]; DX 42, [REDACTED]

¹³ *Id.*

¹⁴ Cloninger Report, ¶ 42.

¹⁵ “Criminals Find a Way to Clone EMV Cards, Decipher, July 31, 2020,” <https://duo.com/decipher/criminals-find-a-way-to-clone-emv-cards> (Last visited October 23, 2024) and “Shimmers: the new credit card skimmers,” WQOW.com, June 29, 2018, https://www.wqow.com/news/shimmers-the-new-credit-card-skimmers/article_8a075616-886b-558d-9a42-8ca5ea3e578f.html (Last visited October 23, 2024).

¹⁶ Cloninger Report, ¶ 31.

¹⁷ “What is Track 1, 2, and 3 Data in Magnetic Stripe Credit Cards?,” Clearly Payments, October 30, 2023, <https://www.clearlypayments.com/blog/what-is-track-1-2-and-3-data-in-magnetic-stripe-credit-cards/> (Last visited October 23, 2024).

42. Chips also do not prevent the other forms of information compromise that the Cloninger Report describes (*e.g.*, phishing, merchant data breaches, other security attacks).¹⁸ EMV chip data can be captured from point-of-sale terminals, and EMV-Bypass Cloning was recognized as a problem by July 2020.¹⁹ As a further example, the December 2020 Nilson Report describes over 250 data breaches in the U.S. alone, resulting in the “ready availability of personally identifiable information (PII) for sale on the dark web,” with the value of annual sales of PII in the \$1 billion range.²⁰ The California State Auditor also found that EDD sent 13 million pieces of mail containing unredacted social security numbers in 2017-18, and at least another 38 million pieces over eight months in 2020, thus “unnecessarily put[ting] claimants at increased risk of identity theft.”²¹ Such information, if intercepted, can be used for identity theft purposes as well as to gain access to and compromise existing accounts. EMV chips would not have protected any of these accounts from compromise.

43. Finally, it is further worth noting that the presence of EMV chips do not prevent physical theft or loss of the card itself.

C. The determination of whether an EMV chip would have prevented skimming or other information compromise requires examination of each particular incident of compromise

44. Because there are a number of ways in which an EMV chip card could have been skimmed or shimmed, or otherwise had its information compromised, it is not possible to conclude that the addition of an EMV chip to a card would have prevented all (or even most) instances of skimming, or all (or even most) instances of information compromise.

¹⁸ Cloninger Report, ¶ 87.

¹⁹ “Criminals Find a Way to Clone EMV Cards, Decipher, July 31, 2020,” <https://duo.com/decipher/criminals-find-a-way-to-clone-emv-cards> (Last Visited October 23, 2024).

²⁰ Nilson Report, Issue 1187, December 2020, Page 5.

²¹ DX 17, Letter from Elaine M. Howle, November 19, 2020, BANA_EDD_MDL-00422776.

CONFIDENTIAL

45. In order to determine whether an EMV chip would have prevented a card from being skimmed, one has to consider the circumstances surrounding the usage of the card at the time that it was skimmed [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

46. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

47. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

48. One would also have to consider whether any of the card readers also had “shimmers” placed in them, [REDACTED]

[REDACTED].

CONFIDENTIAL

49. One must also consider the behavior of the merchant and determine whether the merchant [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

50. Due to the number of considerations, and the fact that EMV chips do not prevent skimming and other forms of card compromise, one must look at the circumstances surrounding a particular compromise in order to assess whether the compromise (whether skimming or another form of compromise) could have been avoided through the addition of an EMV chip.

VI. Adding chips to EDD prepaid debit cards issued by the Bank would not have prevented many of the unauthorized transactions reported to the Bank in 2020

51. In addition to failing to prevent skimming and other forms of compromise, EMV chip cards (1) do not prevent many instances of fraud and (2) would not have prevented all of the unauthorized transactions reported to the Bank. For the reasons discussed in this report, it would not be possible to evaluate how many unauthorized transactions could have been prevented by adding an EMV chip without information about the manner in which each instance of compromise occurred and how each unauthorized transaction was made. Therefore:

- a. Based on my experience overseeing and running a card-issuing business, I strongly disagree with Ms. Cloninger's opinion that chips "would have prevented virtually all card-present counterfeit fraud (including unauthorized ATM withdrawals) for the Bank's EDD debit cardholders at chip-enabled

CONFIDENTIAL

ATMs and POS terminals...”²² Among other things, one would need to examine each instance of reported fraud to determine whether it was first-party fraud (which EMV chips do not prevent), and, if it was third-party fraud, whether such fraud involved the use of counterfeit cards. One would also need to consider any third-party counterfeit fraud that could have occurred even with the presence of an EMV chip, which requires an assessment of the circumstances surrounding each instance of fraud, including whether the PIN was also compromised and whether the ATM or POS terminal at which the fraud occurred was chip-enabled.

- b. As someone who has actually run large card-issuing portfolios, I also disagree with Mr. Regan’s assumption that “EMV chips would have prevented the unauthorized ATM withdrawals that were the subject of Claim Denial and Credit Rescission class members’ claims that triggered the Bank’s CFF Indicator 1...”²³ Mr. Regan’s assumption fails to take into account the various ways that fraud can occur, even if there is an EMV chip on a card. EMV chip card information can still be compromised through skimming, shimming, phishing, or other means, and EMV chip cards can still be stolen. One would need to examine whether each of the ATM withdrawals subject to these claims was actually unauthorized, and if so, whether the circumstances of the fraud were such that an EMV chip would have prevented it, as EMV chips do not prevent all ATM fraud.

²² Cloninger Report, ¶ 14(h).

²³ Expert Class Certification Report of Greg J. Regan, CPA/CFF, CFE, August 29, 2024, Motion for Class Certification, (PX 4, “Regan Report”), ¶ 118

52. Based on my 35 years of experience in the card and payments industry and more than 10 years overseeing what were then the fifth largest credit and debit card portfolios in the United States, these positions expressed in the Cloninger Report and the Regan Report are at odds with the reality experienced in the industry during this time and with the nature of fraud and how it occurs. As explained above, EMV chips are vulnerable to compromise in a number of ways. I explain further below how the addition of an EMV chip to magstripe cards would not have prevented many of the instances of fraud reported to the Bank.

A. The shifting of liability for fraud does not eliminate fraud

53. As a threshold matter, it is important to distinguish between “fraud” and “fraud loss.” The question of whether chips would have prevented *fraud* is different from whether chips would have prevented Bank of America from absorbing the *losses* associated with that fraud.

54. The Cloninger Report describes the liability-shift rules that took effect in October 2015, under which the liability (*i.e.*, financial responsibility) for a fraudulent transaction rested with the party (card issuer or merchant) that did not offer EMV technology.²⁴ These rules were adopted to incentivize the industry to adopt EMV technology, which was a costly undertaking. Pursuant to those rules, the question of whether the card issuer or the merchant was financially responsible for a particular fraudulent transaction depended on whether the card used for the transaction had an EMV chip and whether the merchant required the use of the chip for payment.

55. Thus, under some circumstances, adding an EMV chip to a card may have prevented a fraud *loss* to the issuer by shifting the liability for that loss to the merchant. That is an entirely different question from whether an EMV chip would have prevented the fraudulent transaction itself. In many scenarios, an EMV chip may not have prevented the fraudulent

²⁴ Cloninger Report, ¶ 39.

CONFIDENTIAL

transaction from occurring but may have prevented the card issuer from bearing financial liability for the loss.

56. I address below whether EMV chips would have prevented the transactions that were reported to the Bank as fraudulent, not whether the addition of a chip would have allowed the Bank to shift financial responsibility for those losses.

B. EMV chip cards do not prevent all fraud

57. While adding an EMV chip to a magnetic stripe card can make certain types of card-present fraud more difficult to accomplish, it does not eliminate fraud. Based on my experience in the card and payments industry, there continue to be myriad opportunities for criminals to exploit chip cards. Therefore, it cannot be assumed that the presence of an EMV chip on the EDD prepaid debit cards would have prevented all or even most of the fraud reported to the Bank in 2020-2021.

58. First, chips do not prevent fraud when the reported transactions are not actually fraudulent, such as when cardholders themselves are committing fraud against a bank by falsely reporting unauthorized transactions (first party fraud), or when their report is based on a mistaken belief that the transaction was unauthorized when it was not. Therefore, one cannot conclude that chips would have prevented all of the unauthorized transactions reported to the Bank, including the transactions that involve ATM withdrawals, without considering whether the reported transaction was actually fraudulent, or whether it reflected cardholder fraud or mistake.

59. Second, even as to third-party fraud actually experienced by cardholders (which cannot be identified without first doing a case-by-case assessment to distinguish between first-party fraud or mistake and third-party fraud), EMV chips would not have prevented all of these transactions. As discussed in section IV above, chip cards can still be compromised through

CONFIDENTIAL

skimming, physical theft or loss of the card, or in other ways. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

C. Chips would not have prevented the allegedly unauthorized transactions that involved fraud or mistake by the cardholder

60. Both the Cloninger Report and the Regan Report assume that all reported fraud was, in fact, fraud actually targeting the cardholder. That is an unfounded and implausible assumption. One would have to review each instance of fraud to attempt to determine whether the cardholder actually experienced third-party fraud, or whether the cardholder is committing first-party fraud or made a mistaken report.

61. First, EMV chips do not prevent individuals from committing benefits fraud. Based on review of the materials in this case, as discussed below, there were significant volumes of benefits fraud at the time whereby individuals falsely claimed to EDD, often using stolen identities, that they were entitled to benefits under the EDD program. Many of these same criminals doubled down by subsequently committing fraud against the Bank by falsely reporting unauthorized transactions on their fraudulently-obtained accounts.

62. The California state auditor acknowledged in a January 2021 report that “EDD did not take substantive action to bolster its fraud detection efforts for its UI program until months into the pandemic, resulting in payments of about \$10.4 billion for claims that it has since determined

CONFIDENTIAL

may be fraudulent because it cannot verify the claimants' identities."²⁵ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]"²⁶ Later estimates placed the amount of fraud at \$20 billion (EDD's estimate) to \$32.6 billion (estimate from CEO of Lexis Nexis Risk Solutions).²⁷

63. Based on my extensive experience in the card and payments industry, it is well understood in the industry that EMV chips do not prevent this type of fraud. In such instances, the EMV chip is a technology that would be added to the card issued to an individual who has successfully defrauded the Bank. It does not prevent that individual from using the card and their ill-gotten gains.

64. Second, cardholders may also falsely report that a transaction or transactions were fraudulent; EMV chips cannot prevent these transactions. This includes both cardholders who obtained their cards and accounts fraudulently, as described above, as well as cardholders who were legitimately entitled to the funds in their account. In my experience, fraudulent reports to financial institutions are quite common, and have been for a number of years, including prior to the pandemic. Typically, whenever there is a possibility of receiving funds, fraud is a risk. Many financial institutions are a target for individuals who make such false claims in order to get "free" money. As noted by Socure, a digital identity verification company, in 2023: "[L]osses connected with first-party fraud total more than \$100 billion annually in the U.S. across financial institutions

²⁵ DX 88, CA State Auditor, "Weaknesses in EDD's Approach," January 2021, BANA EDD MDL-00080296

²⁶ [REDACTED]

²⁷ DX 11, "David Manoucheri, "Analysis shows California EDD fraud at \$32.6 billion and counting," KCRA3, October 6, 2022

CONFIDENTIAL

and merchants” and “[a]ll of these loss estimates originate at a single point: when the consumer disputes a transaction.”²⁸

65. This was the very type of fraud evidenced at Bank of America. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]²⁹ He goes on to say: “Upon closer examination, it would appear that someone filed a claim of fraud which was subsequently paid out.”³⁰ EMV chips would not have prevented individuals from either committing benefits fraud, or subsequently filing a false claim of fraud with the Bank.

66. In general, the risk of cardholder fraud is common and known to the industry and not limited to products involved with benefits programs. EMV chips cannot prevent any transactions in which the cardholder is falsely reporting an unauthorized transaction, regardless of who the cardholder is.

67. Third, it is also common for reports of unauthorized transactions from cardholders to involve mistakes even if there is no fraudulent intent; EMV chips cannot prevent these transactions either. For example, a cardholder may report a transaction that they authorized but failed to recognize (*e.g.*, because they do not recognize the merchant name that is listed). I have personally called my bank regarding a transaction I did not recognize on my statement, only to realize the merchant was listed under a name I did not recognize. On other occasions, a cardholder

²⁸ “Socure identity risk insights: Defining and solving the elusive challenge of first-party fraud,” Socure, 2023, <https://www.socure.com/resources/reports/solving-the-elusive-challenge-of-first-party-fraud> (Last visited October 22, 2024).

²⁹ [REDACTED]

³⁰ *Id.*

CONFIDENTIAL

may not realize that another authorized user of their card (*e.g.*, a family member) was responsible for the transaction(s) they are reporting. For example, a March 2022 LendingTree survey indicates that 60% of parents had given their child permission to use their card, and almost half of them later regretted it; and 46% of parents stated their child had made transactions without permission, with the most common instance being in-app or in-game purchases.³¹ Socure reports that 29% of Americans who committed first-party fraud say that it was an accident.³² EMV chips do not prevent these type of transactions from occurring, particularly as, in each of these instances, the person conducting the transaction likely had possession of the physical card.

68. These instances of cardholder fraud and/or error can occur with both ATM and non-ATM transactions. Therefore, one cannot assume, based just on the fact that a card does not have an EMV chip, that a reported transaction was actually unauthorized because it is very possible that a reported transaction involved cardholders themselves committing fraud or making a mistaken report, or cardholders who did not know that another or previously authorized user (*e.g.*, a spouse or child) had used the card to make the disputed transactions.

D. Chips would not have prevented all fraudulent ATM withdrawals reported to the Bank that were actually unauthorized

69. Even as to fraud for which cardholders were the target, EMV chips would not have prevented all of those fraudulent transactions.

70. First, EMV chips would not prevent fraud from occurring on non-chip enabled ATMs.

³¹ “46% of Parents Say Their Child Used Their Credit or Debit Card Without Permission, Racking Up \$500+”, LendingTree, March 1, 2022. <https://www.lendingtree.com/credit-cards/study/kids-and-credit-cards-survey/> (Last visited on October 22, 2024).

³² “Socure identity risk insights: Defining and solving the elusive challenge of first-party fraud,” Socure, 2023, <https://www.socure.com/resources/reports/solving-the-elusive-challenge-of-first-party-fraud> (Last visited October 22, 2024).

CONFIDENTIAL

71. The Cloninger Report acknowledges the existence of non-chip enabled ATMs³³ but does not consider how many of the reported unauthorized transactions involved such ATMs. According to a June 2020 U.S. EMV Migration Summary from Visa, as of the second quarter of 2020, 93% of U.S. ATMs were chip-enabled,³⁴ meaning that 7% of U.S. ATMs still did not require chips. These non-chip-enabled ATMs rely on [REDACTED]

[REDACTED]

[REDACTED]

72. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

73. This is not just a theoretical risk. A FICO blog from March 6, 2024 notes that “the majority of compromises still occur at non-bank ATMs – like free-standing terminals in convenience stores.”³⁵ Likewise, [REDACTED]

[REDACTED]

[REDACTED]

³⁶

74. [REDACTED]

[REDACTED]

³³ Cloninger Report, ¶ 32.

³⁴ VISA U.S. EMV Migration Summary, June 2020, BANA_EDD_MDL-00292669-BANA_EDD_MDL-00292675, at BANA_EDD_MDL-00292673.

³⁵ FICO Blog, March 6, 2024. <https://www.fico.com/blogs/debit-card-compromises-nearly-doubled-2023-fico-data> (Last visited on October 18, 2024).

³⁶ [REDACTED]

CONFIDENTIAL

[REDACTED]

[REDACTED]

75. [REDACTED]

[REDACTED]

76. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

77. Second, the Cloninger Report assumes that all reportedly unauthorized ATM transactions involved a cloned or counterfeit card. However, a cloned or counterfeit EDD prepaid debit card can only be used for an ATM transaction if the person in possession of the card also has the PIN, and the Cloninger Report does not consider whether each of those instances of hypothetical cloning also involved a PIN compromise. As discussed above, skimming or shimmering would not capture the PIN. Also, as the Cloninger Report notes, pinhole cameras and keypad overlays are devices separate from skimmers, and so the skimming of a card for cloning purposes does not necessarily involve a PIN compromise as well.

78. The Cloninger report also does not consider whether any cloned or counterfeit cards resulted from information “skimmed” at a card reader that also had a “shimmer,” such that adding an EMV chip to the card would not have prevented the counterfeiting of the card.

79. The Cloninger Report does not consider whether any of the reported unauthorized transactions to the Bank involved cards that were not skimmed and cloned, for example cards that were physically stolen or lost. In such cases, adding an EMV chip would not have prevented the

CONFIDENTIAL

thief from using the card, as the thief would be in possession of the card (with or without the chip) and could still use it.

80. Lost or stolen cards are a common cause of fraud. For example, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

81. To this point, a January 2016 press release from Experian about a September 2015 survey that the company conducted notes that “15 percent [of survey respondents] keep a written record of passwords and PINs in their purse or wallet or on a mobile device or computer.”³⁷

82. Another study from the University of Cambridge notes that “guessing PINs based on the victims' birthday, which nearly all users carry documentation of, will enable a competent thief to gain use of an ATM card once for every 11-18 stolen wallets, depending on whether banks prohibit weak PINs such as 1234.”³⁸

83. Finally, an RBC study from March 9, 2020 notes that: “55% of Canadians have admitted they've shared their banking PIN or passwords with others.”³⁹ The study also notes that “41% of Canadians have done one or more the following things that could compromise their security:

³⁷ Experian Press Release, January 28, 2016. <https://www.experianplc.com/newsroom/press-releases/2016/data-privacy-day-survey> (Last visited October 18, 2024).

³⁸ “A birthday present every eleven wallets? The security of customer-chosen banking PINs,” University of Cambridge, Joseph Bonneau, Soren Preibusch, Ross Anderson, https://www.cl.cam.ac.uk/~rja14/Papers/BPA12-FC-banking_pin_security.pdf (Last visited on October 18, 2024).

³⁹ RBC Press Release, March 9, 2020. <https://www.rbc.com/newsroom/news/article.html?article=125249> (Last visited October 18, 2024).

CONFIDENTIAL

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] 40

84. In addition, the EDD program itself could have exposed cardholders to potential fraudulent activity. The California State Auditor reported that EDD had put Californians “at risk of identity theft” when it mailed documents containing individuals’ full social security numbers, a practice that took place over a significant period of time, involving at least 51 million pieces of mail sent with information that could be used for identity theft or to access existing accounts.⁴¹

As reflected in [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

42 [REDACTED]

85. As the above examples illustrate, one cannot simply conclude that the presence of an EMV chip would have prevented all fraudulent ATM transactions. One would need to consider

[REDACTED]

⁴⁰ *Id.*

⁴¹ DX 17, BANA EDD MDL-00422774-BANA EDD MDL-00422775.

⁴² [REDACTED]

[REDACTED]

[REDACTED] It also needs to be considered whether the card was lost or stolen. Each of these determinations must be made by looking at the circumstances surrounding each transaction.

E. EMV chips would not have prevented all fraudulent point-of-sale transactions

86. EMV chips also would not have prevented all of the fraudulent point-of-sale transactions. This applies both to transactions that are made with the physical card (card-present transactions) as well as to transactions that do not require use of a physical card (card-not-present transactions). The Regan Report includes in its damages calculations for the purported EMV chip class all unauthorized point-of-sale transactions that are included in the amount of the cardholder's claim filed with the Bank.⁴³ However, neither the Regan Report nor the Cloninger Report consider whether the addition of an EMV chip would have prevented those transactions.

87. Chips provide no protection to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Adding an EMV chip does not stop this process.

88. Chips also do not prevent many card-present transactions. [REDACTED]

[REDACTED]

[REDACTED]

⁴³ Regan Report, ¶ 120.

CONFIDENTIAL

[REDACTED]

[REDACTED].⁴⁴

F. The determination of whether an EMV chip would have prevented a particular unauthorized transaction requires examination of each transaction

89. For all of these reasons, it is necessary to consider the specific facts and circumstances of a particular transaction to assess whether the presence of a chip would have actually prevented that transaction.

90. To determine whether a particular transaction could or would have been prevented by a chip, one would have to first consider whether the transaction was actually fraudulent, or whether it reflects an instance of cardholder fraud or mistake.

91. For any transactions determined to involve third-party fraud, one would next have to consider how the card information was compromised and whether that compromise would have been prevented by a chip. This determination would involve consideration of, among other things,

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].

92. Then, one would have to consider how a fraudulent transaction occurred and whether it would have been prevented by an EMV chip. This determination would involve consideration of, among other things, [REDACTED]

⁴⁴ EMV Bypass Cloning,” Chargebacks911, February 2, 2023, <https://chargebacks911.com/emv-bypass-cloning/> (Last visited October 23, 2024).

CONFIDENTIAL

[REDACTED]

[REDACTED]

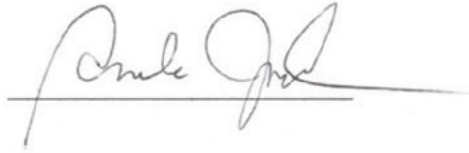
[REDACTED]

VII. Conclusion

93. Based on my more than 35 years of experience in the payments and card industry, it is wrong to conclude that adding chips to cards would have prevented all of those cards from being compromised. Magstripes are still present on chip cards and chip cards can still be susceptible to skimming, shimming, and other forms of information compromise. Therefore the determination of whether a chip would have prevented card information from being compromised must involve a consideration of the circumstances surrounding the compromise.

94. Further, it is wrong to conclude that adding EMV chips to the EDD prepaid debit cards issued by the Bank would have prevented (1) all reports of unauthorized transactions, (2) all reports of unauthorized card-present transactions, or (3) all reports of unauthorized ATM transactions. Ms. Cloninger and Mr. Regan's assumptions do not take into account that (a) not all reported fraud is actually fraud, and (b) chip cards can still be subject to fraud, including card-present and ATM fraud. The determination of whether an EMV chip would have prevented a particular transaction alleged to be fraudulent must involve a consideration of the circumstances surrounding the transaction.

Executed this 24th day of October 2024.



Pamela Ann Joseph

Xplor Technologies
Executive Chair,
April, 2018 to Current

CEO, Xplor Technologies
September 1, 2022 to Current

Xplor Technologies is a global vertical software business that serves Everyday Life Verticals (Fitness, Childcare and Home Services). Xplor also attaches payments for all software clients through its proprietary payments platform. Stepped in (from Chair) to replace CEO after TSG merger. Managed company to 15% growth in revenue in 2023. Effort underway to restructure organization including upgrading talent; centralizing Technology, Ops and Product and building out financial and HR infrastructure to enhance margins.

May 2016 to December, 2017
TSYS
President and COO

TSYS is the largest card issuing processor in the US processing over 55% of all consumer card accounts in North America as well as 90% of all corporate and commercial cards. TSYS is also a top ten processor in the Merchant Acquiring industry and the second largest prepaid card issuer in the US.

As President and COO, responsibility included management of all business lines, establishing and meeting public market expectations, driving revenue growth and margin enhancement as well as oversight of all operational infrastructure. In my short tenure, we exceeded market expectations and the stock price improved by 40%. The company was sold shortly after my departure. Oversight for 11,000 employees.

September 2001 to December 2015
US Bancorp
Vice Chair, Payment Services
CEO, ELAVON

Responsible for all electronic payment business lines including Consumer and Small Business credit, debit and prepaid cards. Responsible for all commercial card solutions, including corporate, purchasing and fleet cards. Responsibility also included global merchant acquiring business serving customers in 27 countries.

During tenure, doubled the size of the business and more than doubled the contribution to the organization. The Payment Services division accounted for over \$5 bil in annual revenue and \$2.5 bil in ebitda. Responsibility included revenue generation, margin enhancement, oversight

of all technology and operational infrastructure (bank was not structured in a centralized environment). Involved extensive M&A, JV partnership formation and retail cobranded partnerships. Expanded the merchant business into Europe, Canada, Mexico and Brazil. Responsible for 9,000 employees

July 1994 to September 2001

**ELAVON (formerly Nova Information Systems)
CEO**

NOVA was founded in 1994. Warburg funded venture. Company went public in 1996 (NYSE). Company grew to become a top five merchant acquirer in the US. NOVA was purchased by US Bancorp in 2001.

Positions held prior to CEO were President and COO, CIO, SVP-Operations, SVP Product and Business Development. Responsible for 2,300 employees.

April 1991 to June 1994

**Visa International
Director, New Market Development**

Responsible for driving Visa acceptance in new markets, primarily the supermarket industry, fast food and other venues such as movie theaters and entertainment venues.

**February 1984 to March 1991
Wells Fargo Bank**

Various positions in Consumer Credit, Debt and Small business solutions. Involvement in the launch of Interlink (on-line debit).

Public Company Boards

Director, Paychex, Inc	2014 to Current	Compensation and Nom/Gov Committees
Chair, Transunion	2015 to Current	Board Chair
		Compensation and Nom/Gov Committees
Director, Adyen	2019 to Current	Audit Committee
Director, Centene Corp	2006 to April 2016	Audit and Compensation Committees
Trustee, Spelman College	2013 to 2020	

Education

University of Illinois Bachelors Degree in Business Administration

Appendix B
CONFIDENTIAL*In RE Bank of America California Unemployment Benefits Litigation***Declaration of Pamela Joseph****List of Materials Considered****1. Expert Reports**

Expert Report of Jane Cloninger in Support of Plaintiffs' Motion for Class Certification dated August 29, 2024

Expert Class Certification Report of Greg J. Regan, CPA/CFF, CFE dated August 29, 2024

2. Case Filings

Plaintiff Second Amended Master Consolidated Complaint dated July 16, 2024

Plaintiffs' Notice of Motion and Motion for Class Certification filed on August 29, 2024

Plaintiffs' Memorandum of Points and Authorities in Support of Motion for Class Certification dated August 29, 2024

3. Depositions and Exhibits

William Matt Martin Deposition Transcript and Exhibits 43-54

Michael Letson Deposition Transcript

Shane Daniels Deposition Transcript

4. Other Produced Documents

BANA_EDD_MDL-00061630-BANA_EDD_MDL-00061632

BANA_EDD_MDL-00073529-BANA_EDD_MDL-00073531

BANA_EDD_MDL-00080294-BANA_EDD_MDL-00080352

BANA_EDD_MDL-00118617-BANA_EDD_MDL-00118618

BANA_EDD_MDL-00151781-BANA_EDD_MDL-00151783

CONFIDENTIAL

BANA_EDD_MDL-00164188-BANA_EDD_MDL-00164190

BANA_EDD_MDL-00292669-BANA_EDD_MDL-00292675

BANA_EDD_MDL-00422774-BANA_EDD_MDL-00422779

5. Publicly Available Documents

Ann Noder, Experian, "Consumers find balance between cyberspace risks and benefits," January 28, 2016, available at <https://www.experianplc.com/newsroom/press-releases/2016/data-privacy-day-survey>

Chargebacks911, "EMV Bypass Cloning," February 2, 2023, available at <https://chargebacks911.com/emv-bypass-cloning>

Chase Bank, Credit Card Marketplace, "What is an EMV chip and how does it store your data," available at <https://www.chase.com/personal/credit-cards/education/basics/what-is-emv-chip-how-it-stores-your-data>

Computer Laboratory, University of Cambridge, "A birthday present every eleven wallets? The security of customer-chosen banking PINs," available at https://www.cl.cam.ac.uk/~rja14/Papers/BPA12-FC-banking_pin_security.pdf

Dawn Papandrea, lendingtree, "46% of Parents Say Their Child Used Their Credit or Debit Card without Permission, Racking Up \$500+," March 1, 2022, available at <https://www.lendingtree.com/credit-cards/study/kids-and-credit-cards-survey/>

Debbie Cobb, FICO Blog, "Debit Card Compromises Nearly Doubled in 2023 – FICO Data," March 6, 2024, available at <https://www.fico.com/blogs/debit-card-compromises-nearly-doubled-2023-fico-data>

Debbie Cobb, FICO Blog, "U.D. Card Skimming Fraud Grows 700+% in First Half of 2022," August 16, 2022, available at <https://www.fico.com/blogs/us-card-skimming-fraud-grows-700-first-half-2022>

EMVCo, "A Guide to EMV Chip Technology," November 2014, available at <https://www.fisglobal.com/-/media/fisglobal/worldpay/docs/insights/a-guide-to-emv-chip-technology.pdf?la=en>

EMVCo, "Enabling Seamless and Secure Contact and Contactless Payments Around the World," September 15, 2022, available at <https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf>

EMVCo, "The Role of the EMV ® Specifications," March 18, 2020, available at <https://www.emvco.com/wp-content/uploads/2022/12/The-Role-of-the-EMV-Specifications.pdf>

CONFIDENTIAL

Europay, Mastercard, and Visa Consortium, Annual Report, 2020, available at <https://www.emvco.com/wp-content/uploads/2022/09/EMVCo-Annual-Report-2020-1.pdf>

Fahmida Y. Rashid, Decipher, "Criminals Find a Way to Clone EMV Cards," July 31, 2020, available at <https://duo.com/decipher/criminals-find-a-way-to-clone-emv-cards>

International Business Machines Corporation, History, "The magnetic stripe," available at <https://www.ibm.com/history/magnetic-stripe>

Kalle Radage, Clearly Payments, "What is Track 1, 2, and 3 Data in Magnetic Stripe Credit Cards?" October 30, 2023, available at <https://www.clearlypayments.com/blog/what-is-track-1-2-and-3-data-in-magnetic-stripe-credit-cards>

KCRA, "Analysis shows California EDD fraud at \$32.6 billion and counting," October 6, 2022, available at <https://www.kcra.com/article/analysis-edd-fraud-326-billion-and-counting/41281662>

Nilson Report, Issue 1187, December 2020

Royal Bank of Canada, News & Stories, "Fifty-five per cent of Canadians admit to having shared their PIN or security passwords with family or friends," March 9, 2020, available at <https://www.rbc.com/newsroom/news/article.html?article=125249>

Socure, "Socure identity risk insights: Defining and solving the elusive challenge of first-party fraud," 2023, available at <https://socure.drift.click/risk-insights>

Tracy Scott, WQOW, "Shimmers: the new credit card skimmers," January 29, 2018, available at https://www.wqow.com/news/shimmers-the-new-credit-card-skimmers/article_8a075616-886b-558d-9a42-8ca5ea3e578f.html

Vicki Hyman, Mastercard, "Swiping left on magnetic stripes," August 12, 2021, available at <https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/>

Note: I also reviewed the materials listed in Appendix B of the Expert Class Certification Report of Jane Cloninger dated August 29, 2024.