EXHIBIT B

REDACTED

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

April 4, 2025

TABLE OF CONTENTS

I. INTRODUCTION 1

II. SUMMARY OF OPINIONS 1

III. STATEMENT OF OPINIONS AND BASIS FOR OPINIONS 5

A. EMV Chips Were the Industry Standard for the Payment Card Industry, Including Prepaid Debit Cards Used to Distribute Government Benefits, by at Least 2019 5

a. By at Least 2019, EMV Was the Card Security Standard for the *Entire* Card Payments Industry 5

b. There Is No Separate Security Standard for "Prepaid Debit Cards." 10

B. The Bank's Decision in Early 2020 to Not Equip EDD Debit Cards with EMV Chips was Inconsistent with Other Participants in the Payments Industry and Subjected Cardholders to a Heightened Risk of Information Compromise and Fraud 17

C. It Would Have Been Feasible for the Bank to Have Transitioned to EMV When the Pandemic Began, and the Bank Has No Supportable Justification for Failing to Do So Until 2021 19

D. EMV Would Have Prevented All or Nearly All of the Unauthorized ATM Withdrawals and Other Unauthorized Card-Present Transactions Class Members Experienced 25

a. The Only Type of Fraud Relevant to this Class is Pin-Enabled, Card-Present Counterfeit Fraud, which EMV is Extremely Effective at Preventing 25

b. EMV Only Type of Fraud Relevant to this Class is Pin-Enabled, Card-Present Counterfeit Fraud, which EMV is Extremely Effective at Preventing 28

c. To the Extent Any Counterfeit Fraud Could Have Nonetheless Succeeded on EMV Cards, the Scope Would Have Been Extremely Limited by Strict Fallback Rules in the Bank's Control 29

d. Individual Inquiries Are Not Necessary to Determine if EMV Would Have Prevented Cardholders' Unauthorized Transactions 32

IV. CONCLUSION 34

Appendix A: List of Additional Materials Considered 25

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").

2. Plaintiffs disclosed my expert report on this matter ("Cloninger Rep.") on March 4, 2025.[1] The same day, Defendant Bank of America, N.A. (the "Bank") disclosed the Expert Report of Pamela Joseph ("Joseph Report"). In this Rebuttal Report, I respond to statements and opinions 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.

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. Many of the opinions expressed in the Joseph Report are misleading, irrelevant, or unsupported by evidence, for the reasons set forth below.

[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.

6. Ms. Joseph's opinion that "it was reasonable for the Bank to issue EDD prepaid debit cards without EMV chips" (Joseph Rep. p.17) is unfounded and ignores relevant evidence about the applicable industry standards, the specific parameters of the Bank's EDD prepaid debit card program (both pre-pandemic and at the outset of the pandemic), and the Bank's own internal cost-benefit analysis favoring EMV chip migration in January 2020.

(a) By at least 2019, the use of EMV chips was an industry-standard security measure for the entire payment card industry, including debit cards used for the administration of government benefits. Joseph's insistence that individual products and program subgroups must be evaluated separately to assess security standards specific to those subgroups is incorrect. From a fraud and card security perspective, payment card industry participants and products are interdependent and should not be examined in isolation – what happens across the payments landscape can change the fraud dynamics of other participants. As the U.S. payments industry achieved large-scale conversion to EMV after the Liability Shift Rules became effective, industry players correctly anticipated that fraud would migrate to products that remained vulnerable to traditional counterfeit fraud, i.e. mag-stripe only cards, and that fraud losses would increase on such programs. Although some programs may not have converted to EMV, the result was sub-industry standard card security for those programs – not an industry with a patchwork of product-specific security standards. Moreover, numerous industry-wide metrics, including the overall transaction volume conducted via EMV technology (over 99 percent on the Visa network), which Joseph does not address, confirm that EMV was the security standard for the overall payments industry by at least 2019.

(b) Even if one were to accept Joseph's premise that different security standards apply to different segments of the payment card industry (they do not), the relevant segmentation would not be "prepaid debit cards," which encompasses a broad range of card products with highly different characteristics. If there were any appropriate sub-industry, it would be prepaid *government benefits* debit cards, many of which migrated to EMV before the rest of the payments industry years before 2019, largely as the result of a 2014 Executive Order issued by President Barack Obama requiring the adoption of EMV for federal benefits cards, described in greater detail below.

(c) Joseph ignores that in early 2020, the Bank itself determined based on its cost-benefit analysis that there was a positive business case for transitioning the EDD debit card portfolio to EMV chip cards, given the size and load value of the portfolio and the rising fraud rate. Even under Joseph's unjustifiably narrow view of "industry standards," there can be no question that, once the Bank determined there was a positive business case to move EDD debit cards to EMV, it was not consistent with industry standards for the Bank then to decline to do so. The Bank's decision at that point not to convert EDD debit cards to EMV, so that the Bank could use such conversion as leverage in its negotiations with EDD, was inconsistent with the actions I would expect to see from a rational and responsible financial institution consistent with industry standards and acting in good faith towards its customers.

(d) Joseph ignores that after the onset of the pandemic, the business case for converting the EDD debit card portfolio to EMV chip cards only grew stronger, as the number of cardholders and total load value increased substantially,

making the program an even more attractive target for skimming and counterfeit card fraud. The Bank's continued failure to issue EMV-chip cards after the onset of the pandemic, even in the face of rising fraud, was inconsistent with the actions I would expect to see from a rational and responsible financial institution acting consistent with industry standards and acting in good faith towards its customers.

(e) Contrary to Joseph's argument that EMV migration in 2020 would have presented insurmountable challenges, in my professional opinion having developed dozens of business cases for EMV migration, which necessarily include forecasting details and costs and benefits of conversion processes, it would have been feasible for the Bank to implement EMV chips during the spring or summer of 2020. Had the Bank done so, it would have averted virtually all the card-present counterfeit fraud at ATMs that class members experienced between the summer of 2020 (the soonest that EMV conversion could have been completed had the Bank begun conversion at the onset of the pandemic in March of 2020) and July 2021, when the Bank finally began issuing EMV chip EDD debit cards.

7. Ms. Joseph's opinion that "[a]dding EMV 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" (Joseph Rep. p.28) is beside the point. In this case, the only relevant unauthorized transactions are unauthorized ATM withdrawals. For all the reasons stated in the Cloninger Report, EMV chips would have prevented most if not all of the unauthorized ATM withdrawals (which are a type of card-present counterfeit card fraud) that EMV Chip class members experienced, as confirmed by the Bank's own documents.

III. STATEMENT OF OPINIONS AND BASIS FOR OPINIONS

A. EMV Chips Were the Industry Standard for the Payment Card Industry, Including Prepaid Debit Cards Used to Distribute Government Benefits, by at Least 2019.

a. By at Least 2019, EMV Was the Card Security Standard for the *Entire* Card Payments Industry.

8. I strongly disagree with Joseph's contention that "Prepaid Debit Cards" is an appropriate way to define the relevant industry for purposes of evaluating the reasonableness of the Bank's failure to issue EMV chip cards to EDD debit cardholders in 2020 and the first half of 2021. *See* Joseph Rep. ¶¶42-47. Rather, the appropriate industry for purposes of determining the applicable card security standard during that time period is the entire payment card industry, for the reasons that follow and those stated in the Cloninger Report. Cloninger Rep. ¶¶46-55.

9. The payments industry is large and diverse but has well-defined boundaries due to various common rules and the interdependency of programs and products. Any participant, including issuers, acquirers, and merchants,[2] that was subject to the Visa and MasterCard Liability Shift Rules announced in 2012 and effective October 1, 2015 (*see* Cloninger Rep. ¶49) would be considered part of the payments card industry, regardless of the size or type of product offered.

10. The liability shift rules apply to all products and programs, issuers and acquirers/merchants, in the payment industry as specified by the brand (Visa, MasterCard, etc.) on the card. If there is a Visa or MasterCard brand on the card, the liability shift applies.

11. Joseph correctly notes that the liability shift rules did not "include any requirement for card issuers to implement EMV chip technology." Joseph Rep. ¶27. Industry participants understood that the migration to EMV was up to each participant and not required. Still, industry participants also knew that by deciding not to migrate to EMV by the liability shift

[2] These terms are defined in the Cloninger Report at ¶7 n.3.

effective date (October 2015), their program would be subject to liability for any fraudulent card-present counterfeit transactions. This is why the rules did, in fact, operate as a "primary catalyst" for EMV adoption across the industry, as Joseph concedes. *See* Joseph Rep. ¶26.

12. While the risk of liability for card-present counterfeit fraud might have been small prior to the conversion of larger programs, when larger programs converted, industry participants knew fraud would migrate to programs that remained the weakest link, i.e. mag-stripe only cards, and that fraud losses on those weaker security programs would increase. *See* Cloninger Rep. ¶¶79-83.

13. This dynamic, in which the decisions of some payments actors affect the rational calculations of others, reflects that the products and programs that make up the payments industry are interdependent. Payment cards cannot function without issuers to provide cards to the cardholders and without acquirers to process the card transactions that merchants accept for payment. This interdependence is precisely why the liability shift rules are broad-reaching and effective—they recognize that each actor can make its own decision based on its own business case *and* provide incentives for everyone to migrate by re-allocating the risk for fraud between different actors to those who have chosen not to adopt EMV.

14. The best and highest target for fraud at any given moment is dependent upon the actions of the rest of the industry. As I discuss more fully below, the only type of fraud that EMV was designed to address and that the technology affects is card-present counterfeit fraud. As EMV is implemented, initially card-present counterfeit fraud migrates among the participants that have not yet converted, but the overall card-present counterfeit fraud levels do not begin to drop. Once a tipping point is reached wherein enough EMV cards and merchant EMV acceptance points have converted, particularly with larger, high-value programs converting to EMV, card-present counterfeit fraud levels associated with card-present counterfeit fraud begin

to decline within the market. *See* Cloninger Rep. ¶44 (detailing the decrease in fraud with EMV implementation worldwide). At the same time, fraudsters will move down the value chain to target smaller programs that previously had been under their radar or not worth the trouble of targeting, but that now present the easiest and most-available targets for fraud. It is often at this point, when fraud attacks are funneled to previously low-value target programs, that those programs will undergo EMV conversion.

15. Elimination of card-present counterfeit fraud through broadscale EMV migration is thus dependent upon the actions of the entire industry. Analyzing smaller programs in isolation from larger programs improperly ignores the relationship between those programs and the industry-wide effects of EMV conversion by other actors, serving only to obfuscate the impact of a change in the larger programs for security standards on the industry as a whole.

16. Looking at the entire industry, particularly its infrastructure and some of its largest and most important participants (e.g. Visa), EMV was very broadly adopted within the U.S. by 2019. As detailed in the Cloninger Report and summarized again below, critical metrics for the market reflect that broad adoption. *See* Cloninger Rep. ¶¶50-54.

17. Beginning, first, with ATM and Point-of-Sale ("POS") adoption rates: By early 2018, 91% of all U.S. ATMs had converted to EMV-enabled ATM terminals to service EMV-enabled debit and credit cards.[3] ATMs had been slower to convert due to technical requirements that made migration more complex, but by 2018 that process was largely complete. Visa additionally reported that as of June of 2019, 80% of all storefronts in the United States accepted EMV-chip cards.[4] These high ATM and POS adoption rates are important to measuring the

[3] *See* Cloninger Rep. ¶54 (citing Nearly All US ATMs Now EMV-Capable, Study Finds, ATM Marketplace (April 6, 2018), https://www.atmmarketplace.com/news/nearly-all-us-atms-now-emv-capable-study-finds/).

[4] Visa, Visa Chip Card Update (June 2019), https://usa.visa.com/content/dam/VCOM/blogs/visa-emvchip-infographicQ2-080819-v2a.pdf.

overall shift to EMV in the industry because they represent necessary infrastructure to a near-total EMV conversion and create pressure under the liability shift rules for all other actors to convert to EMV or risk broad liability for any fraud. More simply, without places to use EMV cards, there would be no EMV transactions.

18. A second critical metric for determining industry-wide standards is overall transaction volume, i.e., the total dollars of the aggregate transactions conducted with payment cards. By March 2019, 99% of Visa's total U.S. payments volume ($81B) was completed using an EMV chip card.[5] Visa's transaction volume matters as a measure of the industry's behavior because, in order to achieve this milestone, the large majority of active cards and the majority of POS/ATM acceptance locations had to be converted to EMV, *and* consumers had to be using their chip cards—an important trifecta measurement of the industry. That Visa, one of the leading and largest industry brands, saw such universal usage of EMV technology by early 2019 indicated that a major shift in the U.S. payments market had been completed. That conversion would also have wrought major implications for all other smaller programs and products that had not yet converted to EMV in 2019.

19. Thus, by early 2019, all of the infrastructure necessary for EMV (including sufficient ATM and POS locations) was in place, consumers were actively engaging in its use, and shifting fraud trends would have been changing the business cases for EMV conversion even for smaller programs and products.

---

[5] *See* Cloninger Rep. ¶54, citing Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent, VISA (May 28, 2019, 3:28 PM), https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html; EMV in the U.S. (2020 Update), Thales (2020), https://www.thalesgroup.com/en/americas/united-states/digital-identity-and-security/emv; *see also* Understanding the U.S. EMV Liability Shifts, US Payments Forum at 4 (July 2017), https://www.uspaymentsforum.org/wp-content/uploads/2017/07/EMV-Fraud-Liability-Shift-WP-FINAL-July-2017.pdf.

20. Notably, Joseph does not refute that EMV had reached broadscale acceptance by 2019. *See* Joseph Rep. ¶¶33-34. Joseph notes that the "change in card payment network rules in October 2015 did not result in adoption of EMV chips across all cards and all products," *see id.*, but that does not change the fact that EMV had already become the well-established industry standard by at least 2019. That there are some market participants who deviate from the industry standard does not destroy the existence of the standard.

21. Joseph notes data from EMVCo, the organization responsible for managing the EMV standards, to suggest that EMV adoption in 2019 was lower than the metrics above demonstrate. Joseph Rep. ¶¶33-34. EMVCo tracks two indicators of EMV conversion: the percentage of cards in circulation that are EMV-enabled and the percentage of overall transactions (by count) that are conducted with EMV cards. EMVCo numbers include cards and transaction counts across all major brands including JCB, Discover, Union Pay, as well as MasterCard and Visa. Joseph focuses on the percentage of cards issued in the United States in 2020 and 2021 that did not contain EMV chips (37%). *See id.*

22. It is important to stress that EMVCo data is based on the percentage of the total *number* of transactions while Visa's 2019 total transaction volume, discussed above, is based on the percentage of the total *dollar value* of those transactions. *See supra* ¶¶18, 21.

23. In my view, the most meaningful of the three metrics is the percent of card-present dollar volume conducted via EMV in the United States as reported by Visa. As noted above, this metric better represents the interconnection between merchant acceptance locations and actual deployment of *active* cards which results in dollar purchase volume that is processed via EMV.[6] The dollar value reflects a higher percentage of EMV usage because the U.S.

[6] Indeed, one potential explanation for the elevated percentage of total cards without EMV in 2019 is the continued possession of inactive mag-stripe only cards by cardholders. *Cf.* Board of Governors of the Federal Reserve System, Credit Card Profitability (Sept. 9, 2022),

merchant rollout concentrated on higher-dollar locations first, a strategy that enabled the bulk of the volume to be protected by EMV while the remainder of the industry completed converting to EMV and most U.S. issuers concentrated their rollouts on their *active* card bases. As discussed above, higher-value conversion is important both because it plays an important leadership role in the industry and because it shifts fraud activity to lower-dollar targets and further incentivizes broadscale conversion.

b. There Is No Separate Security Standard for "Prepaid Debit Cards."

24. Even if one were to try to define the relevant industry as something less than the entire payment card industry for purposes of assessing the reasonableness of the Bank's failure to issue EMV chip cards to EDD debit cardholders in 2020 and the first half of 2021, "Prepaid Debit Cards" is not an appropriate way to define the relevant sub-industry, as there is no greater homogeneity among "prepaid debit cards" as a category than there is among payment cards at large.

25. "Prepaid debit cards" encompasses a wide-ranging and heterogeneous body of products. Joseph's analysis of "prepaid debit cards" appears to include, per her definition, any card "with access to funds that have been pre-loaded on to the card" and that "are not linked to any checking or savings account" and that can typically "only receive funds from a single designated source." Joseph Rep. ¶29(iii).

26. The Consumer Financial Protection Bureau ("CFPB"), however, observes that cards fitting that description "have different features, functions and fees" and can include cards as diverse as reloadable prepaid cards, non-reloadable prepaid cards, payroll cards, government

---

https://www.federalreserve.gov/econres/notes/feds-notes/credit-card-profitability-20220909.html (noting that 16 percent of credit card accounts are inactive).

benefits cards, college ID cards, gift cards, and more.[7]

27. For many reasons, it is not appropriate or meaningful to group together all "Prepaid Debit Cards" and suggest that they share common characteristics that give rise to a distinct "industry" security standard separate and apart from the overarching security standard that applies to the industry comprised of all payment cards.

28. Prepaid cards differ by card type: for example, "open-loop" verses "closed-loop" prepaid cards.[8] Open loop cards generally are associated with a major brand, like Visa or MasterCard, and can be used anyplace where those brands are accepted. On the other hand, closed loop cards are accepted only at specific merchants associated with the merchant that issued that card. Frequency of use, delinquency rates, and fraud rates vary between these two categories.

29. Prepaid cards also differ based on their ability to be reloaded with additional funds. The difference between reloadable and non-reloadable prepaid debit cards for card security analyses cannot be overstated. Non-reloadable cards, which include prepaid gift cards, are generally anonymous or quasi-anonymous, meaning they do not contain personal data in their mag stripes that can be compromised. Reloadable prepaid cards, by contrast, contain the same type of mag-stripe data as non-prepaid debit cards and credit cards.

30. Prepaid cards additionally differ by use of the card. Some prepaid debit cards are used for specific industry transactions, such as transit, tolls, or mobile phones. Others are used to replace income for retirees or unemployed individuals such as Social Security, veterans' benefits and unemployment benefits. Still others are used for low-income assistance and may have specific use restrictions and different regulatory oversight, such as Electronic Benefit Transfer ("EBT") cards, used to administer Supplemental Nutrition Assistance Program ("SNAP")

---

[7] Consumer Financial Protection Bureau, Choose the Right Card For Your Situation, https://www.consumerfinance.gov/consumer-tools/prepaid-cards/choose-the-right-card/ (last accessed March 25, 2025).

[8] *See* Julia Kagan, Closed Loop Card: Definition, How it Works, vs. Co-Branded Card (March 7, 2024), https://www.investopedia.com/closed-loop-card-definition-4683996.

benefits.[9]

31. EDD debit cards are reloadable prepaid debit cards loaded with income-replacement funds, which for many unemployment insurance recipients are subsistence funds on which they depend for their essential living expenses while unemployed. EDD debit cards are typically reloaded on a regularly recurring (biweekly) basis with substantial sums of money; the weekly UI benefit amount is approximately 50% of the recipient's weekly earnings prior to becoming unemployed, capped at $450 per week, and according to a 2022 study by the California Legislative Analyst's Office, the average UI benefit payment is approximately $330 per week.[10] EDD debit cards are issued to a particular recipient, and the mag-stripe on the cards contains and stores personal cardholder information.

32. Because of these features, EDD debit cards share more in common with Direct Express prepaid debit cards issued by the federal government and other reloadable, individualized prepaid cards used to disburse income-replacement government benefits, than they do with other types of prepaid debit cards, such as non-reloadable prepaid cards, college ID cards, and gift cards. These features are far more relevant to determining what type of security standard should apply to a card than the simplistic question of whether it is a "prepaid" or "non-prepaid" card.

33. Accordingly, if one were to try to define the relevant industry as something less than the entire payment card industry for purposes of assessing the reasonableness of the Bank's failure to issue EMV chip cards to EDD debit cardholders in 2020 and the first half of 2021, the relevant industry would be prepaid government benefits cards, i.e., one would exclude certain non-analogous prepaid debit cards, such as gift cards and other non-reloadable cards, closed loop

[9] U.S. Department of Agriculture, What Can SNAP Buy?, https://www.fns.usda.gov/snap/eligible-food-items (last accessed April 3, 2025) (detailing restrictions on use of SNAP funds).

[10] *See* Legislative Analyst's Office (LAO), State of California and Gabriel Petek, Improving California's Unemployment Insurance Program, LAO, 6 (Aug. 2022), https://lao.ca.gov/reports/2022/4615/Improving-CA-UI-Program-080822.pdf.

cards, and other special-purpose use cards.

34. The most analogous program is the federal government's Direct Express program. Direct Express federal programs provide prepaid debit cards for monthly deposits of Social Security, Supplemental Security Income, veterans' assistance, and other federal benefits that are administered by the Treasury Department, as well as debit payment cards provided through the General Services Administration (GSA).[11] *See* Cloninger Rep. ¶53. By 2019, all Direct Express prepaid debit cards issued by the federal government had EMV chips, as a result of the Executive Order signed by President Obama in 2014 mandating that all federal benefits payment programs convert to EMV in order to provide enhanced security for benefits recipients.[12]

35. Joseph's reliance on a 2022 Federal Reserve's Depository and Financial Institutions Payments Survey ("Federal Reserve Study" or "Study") to argue that mag-stripe only cards were prevalent among prepaid debit cards in 2019 and 2020 is misplaced for the same reasons provided above that "prepaid debit cards" encompass a heterogenous mix of cards, many of which are not analogous to EDD debit cards. Joseph Rep. ¶¶45-46.

36. The survey-based study requested participants to provide data relating to all types of "general-purpose" prepaid cards, including both reloadable and non-reloadable cards, gift cards, payroll, refund and customer incentive cards, and even virtual cards.[13] As explained above, there are many types of prepaid debit cards that do not share relevant characteristics with EDD debit cards for purposes of assessing the reasonableness of card security features, such as whether the card is reloadable, whether it is regularly reloaded with funds, whether the card is loaded with funds on which the cardholder reasonably expects to be able to rely for their basic living expenses, whether the load value of funds is more than de minimis, whether those funds

---

[11] *See* Direct Express, Frequently Asked Questions, https://www.usdirectexpress.com/faq.html (last accessed Aug. 8, 2024).

[12] *See* Cloninger Rep. ¶53, Exec. Order No. 13681, 79 F.R. 63491, §1 (Oct. 23, 2014).

[13] Joseph Rep. Appendix C, p. 1-2, citing the Federal Reserve Payments Study Glossary Survey Period: Calendar Year 2022, pp. 4, 39.

can be transferred to other accounts, and whether access to the card can give a fraudster access not only to the cardholder's funds but also to the cardholder's sensitive personal information. Data about "prepaid debit cards" generally, without disaggregating between the different types of prepaid debit cards, does not shed light on whether EMV chips were the accepted industry standard by at least 2019 for prepaid government benefits cards.

37. Additionally, I note that Joseph's report does not provide any information on which participants responded, overall response rates, or other information that would help one understand the significance of the study's findings. Indeed, even the geographic scope of the study is absent in the Joseph Report body and Appendix C. Although many studies explicitly discuss their own limitations, no such discussion has been included in Joseph's excerpts of the 2022 Study.

38. Regardless of the Federal Reserve Study, Joseph principally concludes that EMV cards were not industry standard for (all) prepaid debit cards based on several "distinctly lower-risk characteristics" that she argues make EMV conversion for prepaid cards uneconomical. Joseph Rep. ¶¶42-44. The two characteristics to which Joseph points are: (1) lower balances and fewer available funds and (2) no tie to consumer checking or savings accounts or lines of credit. Joseph Rep. ¶43.

39. I disagree with Joseph's conclusion that these factors inherently lead to low-risk portfolios for fraud. Indeed, Joseph's analysis of these factors completely ignores the foreseeable outcome of the impact of migration of those other parts of the market to EMV: that fraud would migrate to the remaining pockets of unprotected, less secure programs, i.e., those that remained mag-stripe only. By 2019, fraud had begun to target smaller mag-stripe only card programs, even those with lower balances and no access to additional funds, because they were easy marks and provided quick access to cash compared to other types of fraud. *See infra* ¶¶44-45, 95.

40. As discussed in the Cloninger Report, the payments industry had been warning of this exact fluctuation in fraud to mag-stripe only card programs for years. *See* Cloninger Rep.

¶¶79-83.

41. It is clear that by at least 2019, the market situation for prepaid government cards had changed. No longer were such programs too small with load values too low to be unattractive to criminals. These shifts within the broader payments industry would have dramatically impacted EMV business cases for these programs despite smaller load values, shorter terms, and other characteristics specific to unemployment benefit cards, nullifying historical assumptions about the "security" of these smaller programs. These shifts in the market should have been reevaluated and incorporated into the business case as soon as evidence of the shifts emerged.

42. Joseph's analysis is additionally incomplete because it fails to account for the inherent value and attraction of ATM-enabled prepaid debit cards (like the EDD portfolio) to fraudsters. Some prepaid cards Joseph includes in her analysis are "closed-loop," meaning they can only be used at a particular retailer or location, and many cannot be used at ATMs.[14] But government benefits prepaid debit cards are able to be used *at ATMs*. Any product that is cash or near-cash is highly attractive to criminals whose ultimate goal is to steal cash—not merchandise that has to be converted to cash. Thus, ATMs are prime targets for criminals, and programs like mag-stripe only debit cards, even if they are low balance and limited in access to additional funds, provide easy access to that cash.

43. Equally important, Joseph ignores the qualitative factors that are important in evaluating the EMV business case for prepaid debit cards, more generally. In addition to the costs and benefits that can be quantified (including fraud loss forecasts, incremental cost of chip cards, investment and benefit timing, costs for employee and customer training and

[14] *See* Julia Kagan, Closed Loop Card: Definition, How it Works, vs. Co-Branded Card, Investopedia (March 7, 2024), https://www.investopedia.com/closed-loop-card-definition-4683996.

communication, and other quantifiable data elements), there are qualitative benefits associated with EMV including the customer experience, ubiquity of acceptance, trust and network reliability and security of the payment system. Payment systems are built on consumers' trust that their payment card will work and that their funds are secure. The customer experience must be consistent and provide reliable access to the customer's funds. In many of the early conversions to EMV, these qualitative considerations drove the business case forward despite high costs and unattractive quantifiable considerations.

44. Joseph also generally does not address the 2014 Executive Order and its import for assessing the industry standard for government benefits cards. The fact that the federal government required prepaid debit cards administering federal benefits to be issued with EMV chips by 2015 created a sea change that cannot be ignored, particularly from a qualitative perspective. Any government benefits program that did not issue EMV-chip prepaid debit cards after 2015 would have been out of step with federal government benefits cards in this sub-industry and, by 2019, would have placed its cardholders (and government benefits beneficiaries) in the direct line of fire for fraud trends shifting to mag-stripe only cards.

45. Without taking into account these additional factors – shifting fraud targeting even smaller, low-value programs, the particular attractiveness of ATM cards to fraudsters, and qualitative factors favoring EMV conversion for government benefits programs, in particular – Joseph's analysis of the industry standard is woefully incomplete. In my view, it is inappropriate to sub-segment the payments industry when evaluating the business case for EMV. As in all business cases, one must look to the broader industry and incorporate trends into the forecasts and assumptions upon which the analysis rests. When evaluating EMV, one would have to have blinders on to not incorporate the broader industry migration to EMV and the foreseeable shifts in fraud patterns that would result.

B. The Bank's Decision in Early 2020 to Not Equip EDD Debit Cards with EMV Chips was Inconsistent with Other Participants in the Payments Industry and Subjected Cardholders to a Heightened Risk of Information Compromise and Fraud.

46. To the extent that Joseph's conclusion that the Bank's decision to issue EDD cards in 2020 without EMV chips was "reasonable" largely echoes her industry-standard analysis for prepaid debit cards above, her conclusion is subject to the same critiques set forth above. Joseph Rep. ¶¶48-49. Joseph concludes the Bank's issuance of mag-stripe only EDD cards was reasonable because (1) the cards had low balances; (2) the EDD program benefits were typically short-term; (3) the EDD program size was "modest" prior to the pandemic; (4) EDD cards were "generally not a target for fraud" before the pandemic; and (5) EMV was not industry-standard security for prepaid cards. Joseph Rep. ¶48. Joseph repeatedly concludes that the program had "less fraud risk" as a result of these characteristics. *Id.*

47. For reasons both theoretical and *based in Bank analysis* in 2019 and 2020, I disagree with Joseph's conclusion that the EDD portfolio was not a risk for fraud even before the onset of the pandemic.

48. First, Joseph is incorrect that a small program with low values would, in 2019 or 2020, still have benefited from falling below the radar of fraud rings. Joseph's analysis fails to consider or even address the broad industry consensus that predicted and then observed increasing fraud on smaller, low-value mag-stripe only programs as a result of wider EMV adoption by larger programs. *See supra* ¶¶12-14; Cloninger Rep. ¶¶79-83. Thus, her conclusion that the EDD portfolio's "modest" size and comparatively low value loads would inherently make it less attractive to fraudsters is unsupported and, indeed, contradicted by industry fraud trends in 2020. Moreover, Joseph again ignores that mag-stripe only prepaid debit cards have a

particular intrinsic appeal to criminal groups in the easy access the cards provide to cash via the ATM.

49. The Bank was aware of these trends and would have factored them into the business case it developed for EMV in 2020. Indeed, the Bank acknowledged in a presentation dated January 27, 2020, that "[a]s high-value debit and credit cards (where higher card spend justifies higher-cost fraud deterrence) have migrated to EMV technology, *fraudster attention has migrated to mag stripe only cards (like EDD), driving up sustained fraud loss rates >50%.*"[15] That Joseph's analysis nonetheless excludes the increasing fraud on smaller mag-stripe only programs, including the EDD portfolio, significantly undercuts the credibility of her conclusions.

50. Moreover, nowhere does Joseph acknowledge that the Bank conducted its own analysis of all these factors in January 2020 regarding the EMV conversion and concluded that conversion *was warranted*. Cloninger Rep. ¶¶60-63. A cost-benefit analysis that the Bank prepared on or about January 10, 2020 showed that the incremental cost of adding an EMV chip to its EDD debit cards was only approximately [redacted] per card.[16] The head of the Bank's EDD debit card product team, Brad Garfield, in an email dated January 10, 2020 stated: "In the first year, the worst case is that we have about $500k in added plastic cost before we start to see any fraud savings. Though in practice we will avoid some fraud from day 1. *The model still makes sense to move.* Breakeven in year 2, notable savings by year 3."[17] *See* Cloninger Report ¶¶62-65. Thus, prior to the pandemic, the Bank's *own internal analysis* concluded that there was a positive business case for migrating the EDD portfolio to chip *before* the pandemic began.

51. The Bank's resulting decision to ignore its analysis of the factors Joseph details features nowhere in her report, nor could she defend such a decision as reasonable. Indeed,

---

[15] BANA_EDD_MDL-370150 at -370154 (emphasis added).

[16] *See* BANA_EDD_MDL-351839 at -351839–40. A later cost-benefit analysis conducted by the Bank in mid-late 2020 determined the incremental unit cost of adding EMV chips to EDD debit cards to be even lower, only $0.36 per card. *See* BANA_EDD_MDL-104742 at -104744.

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

documents produced by the Bank in this litigation indicate that the Bank ignored its own internal business case in early 2020 solely because the Bank decided to use EMV chips as bargaining leverage to try to extract contractual concessions from EDD (elimination of EDD's revenue share under the contract).[18] *See* Cloninger Report ¶¶68-71.

52. The Bank's decision to issue mag-stripe only EDD cards, notwithstanding its own positive business case and industry conditions in 2020, deviates materially from the behavior I would expect from a sophisticated financial institution acting in good faith to uphold its commitment to cardholders. Joseph's defense of the Bank's decision as "reasonable" is flawed and ignores the Bank's own understanding of industry-wide and EDD-specific trends.

53. Finally, Joseph incorrectly states that the Bank "needed EDD's approval to convert to EMV chip technology." Joseph Report ¶41. Joseph's unsubstantiated assertion does not consider, and is inconsistent with, certain documents produced by the Bank. Specifically, Joseph's assertion is inconsistent with the EDD's letter to the Bank dated March 13, 2021, in which EDD expressly rejected language the Bank had proposed including in a letter agreement between the Bank and EDD regarding issuance of EMV chip cards that suggested EMV chip cards were not previously authorized under the EDD-Bank contract. The EDD responded that it did not believe such language, or even a formal letter agreement, was necessary, because the issuance of EMV chips was consistent with the existing contract language, which had always permitted the Bank to issue EMV chip cards.[19]

C. It Would Have Been Feasible for the Bank to Have Transitioned to EMV When the Pandemic Began, and the Bank Has No Supportable Justification for Failing to Do So Until 2021.

54. Contrary to Joseph's contentions, migration to EMV was feasible, even during the first months of the pandemic. Joseph Rep. ¶¶15, 58-64, 125.

---

[18] *See* Ex. 27 at -351839-40; Ex. 108 at -102937; Ex. 28 at -116001; Ex. 24 at -123235.

[19] *See* BANA_EDD_MDL_59312 at -59312 (detailing EDD's view that amendment to the EDD-Bank contract to implement EMV migration was not "necessary" because "there is nothing in the contract precluding this – *in fact the contract supports such a move*" (emphasis added)).

55. Joseph cites two reasons for the supposed infeasibility of an EMV conversion: (1) ambiguous delays and disruptions and (2) a global card shortage. Neither justifies the Bank's failure to issue EMV chip cards to EDD debit cardholders until July 2021.

56. The lead time for executing an EMV conversion can be several weeks, and full implementation can take 14-17 weeks. However, Joseph ignores that had the Bank begun the migration in March 2020, when it was clear that the EDD program would be expanding exponentially over the coming year, even allowing for the necessary 14-17 week migration period, the migration would have been completed before June or July of 2020, averting much of the fraud going forward. Notably, the Bank would have been able to leverage knowledge gained in the conversion of its commercial card portfolios five years earlier.

57. Joseph focuses on "disrupt[ions]" that would have been caused by the regular components required for EMV conversion, including designing new card package materials, training Bank employees, and enacting changes to fraud tools. Joseph Rep. ¶61. But the 14-17 week time period includes the time for these elements. These changes are part of any well-executed EMV migration—not impediments to the ability to migrate.

58. Nor were these basic elements of EMV conversion made infeasible by the challenges and conditions of the pandemic. Joseph ¶59. Bank of America is the largest issuer of commercial debit cards and one of the largest issuers of credit cards in the U.S., all of which have been issued with EMV chips since 2015. The Bank would have had time-tested vendor relationships for card production with vendors and processes capable of generating millions of cards in order to service the Bank's card production demand for its commercial customers. Just as the Bank worked with EDD and its vendors to scale up the mag-stripe card production, one would expect the Bank to have been able to work with its EMV card production processes and

experienced vendors to scale up the migration to EMV and meet the increased demand for EDD cards.

59. Card production does not have the same labor constraints as other support functions, like call centers, and thus would not have similar pandemic related staffing problems. Card production is a highly automated process which requires a minimum of human intervention compared to, for example, call centers.

60. Despite Joseph's discussion of the certainty of "disruptions" an EMV migration would have caused, she cites nothing indicating that the Bank even considered any of these options to leverage existing bank vendor relationships and EMV capabilities, and I am not aware of any such documents.

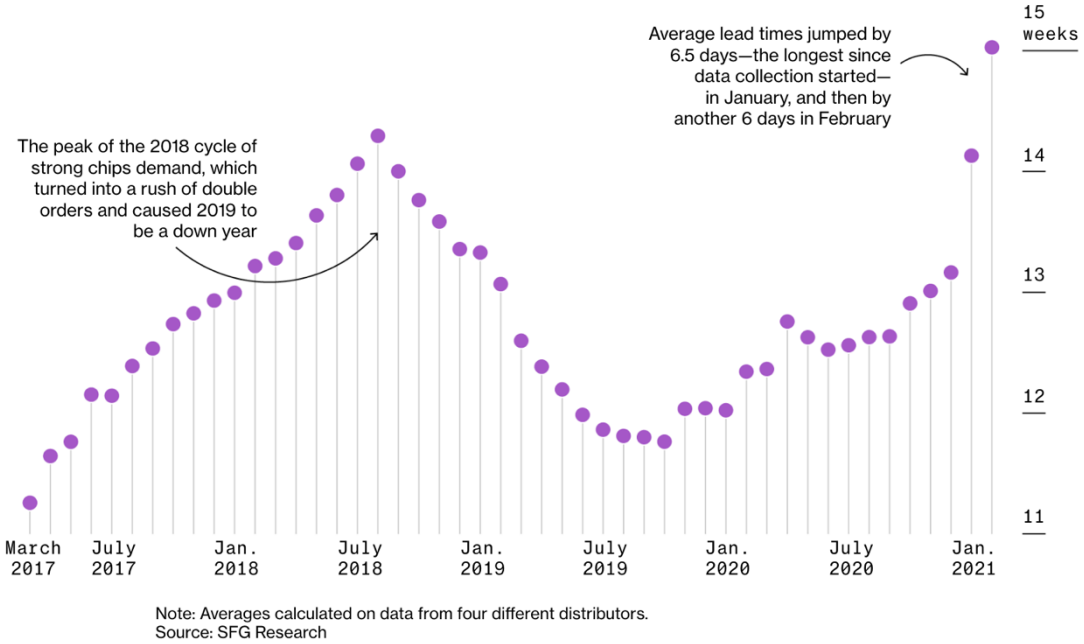
61. It is also unlikely that the Bank's card production would have been disrupted by any chip shortage resulting from supply chain disruptions during the pandemic, as Joseph suggests. Joseph Rep. ¶63 Although the chip shortage began even before the pandemic, the crunch in chip availability affecting card issuance did not hit until 2021.[20] Before then, Bloomberg reported that several leading chip providers had retained lead times under 14 weeks throughout 2020.[21] Indeed, the Bloomberg visual below demonstrates that lead times in 2020 never increased beyond 14 weeks.

---

[20] *See* Ian King, Debby Wu, & Demetrios Pogkas, How A Chip Shortage Snarled Everything From Phones to Cars, Bloomberg (March 28, 2021), https://www.bloomberg.com/graphics/2021-semiconductors-chips-shortage/; Up to 1 Billion Payment Cards At Risk of Not Being Issued As Chip Shortage Impact Looms Over the Payment Cards Industry, ABI Research (Aug. 5, 2021), https://www.abiresearch.com/press/1-billion-payment-cards-risk-not-being-issued-chip-shortage-impact-looms-over-payment-cards-industry.

[21] *See* Ian King, Debby Wu, & Demetrios Pogkas, How A Chip Shortage Snarled Everything From Phones to Cars, Bloomberg (March 28, 2021), https://www.bloomberg.com/graphics/2021-semiconductors-chips-shortage/.

Patiently Waiting: Lead Times for Chips Surpassed Their 2018 Peak in February[22]



62. ABI research similarly reported that the chip shortage did not impact 2020 and only became a factor by mid-2021: "Although the chip shortage impact has remained largely invisible through the first half of 2021, with the impact counterbalanced somewhat by existing stock levels, it is beginning to become very visible in the second half of 2021. As the lead times from chip order to delivery continue to lengthen, 2022 should be considered the critical chip shortage impact year."[23] Finally, in an interview with BCS (the chartered institute for IT), Gartner analysts reported that the chip card shortage started in early 2020 in conjunction with the

[22] *Id.*

[23] Up to 1 Billion Payment Cards At Risk of Not Being Issued As Chip Shortage Impact Looms Over the Payment Cards Industry, ABI Research (Aug. 5, 2021), https://www.abiresearch.com/press/1-billion-payment-cards-risk-not-being-issued-chip-shortage-impact-looms-over-payment-cards-industry.

pandemic and peaked in the second quarter of 2021, returning to normal only a year later in the second quarter of 2022.[24]

63. It is telling that the Bank was able to implement EMV within its stated timeframe of 14-17 weeks despite the fact that the chip shortage was at its peak during this 2021 time period.[25] And the Bank migrated the EDD portfolio to EMV in mid-2021, at the peak of the shortage and within the Bank's expected timeframe, apparently without any "disruption" to cardholders. If the Bank could migrate the portfolio at the peak of the chip shortage, it should have been able to migrate prior to the peak as well.

64. I further disagree with Joseph that "the actual timeline by which the Bank implemented chips into the EDD Prepaid Debit cards" – *initiating* almost a full year after the pandemic began – "was reasonable." Joseph Report ¶64. The Bank should have started the implementation process at least when its updated business case demonstrated, in the Bank's own words, that it "ma[de] sense to move" to EMV. Cloninger Report ¶64. That the Bank waited almost a year *after* the pandemic began to begin EMV migration is even less defensible.

65. Looking to Joseph's own criteria, including the size of the EDD portfolio, the value loads, and the resulting risk of fraud targeting EDD cards, the Bank's business case would have been even more compelling after the onset of the pandemic. The size of the program was predicted to increase exponentially both in terms of number of unemployment beneficiaries and the dollar value of those benefits, as Joseph details. Additionally, the length of time that a beneficiary could collect unemployment was extended during the pandemic.[26] These changes

[24] Understanding the Global Chip Shortage, BCS (March 3, 2023), https://www.bcs.org/articles-opinion-and-research/understanding-the-global-chip-shortage/.
[25] Joseph Report ¶64. EDD approved in March 2021 and the Bank began issuing EMV cards in July 2021, four months later.
[26] California Employment Development Department, California Unemployment Benefits Programs, https://edd.ca.gov/siteassets/files/unemployment/pdf/benefit-flowchart.pdf (last accessed April 2, 2025) (describing pandemic extensions to eligibility of unemployment benefits).

made the program an even more attractive target for criminals. It was highly foreseeable that these factors would make the program much more attractive to fraud rings, particularly as counterfeit card-present fraud was already increasing in the portfolio, triggering the Bank's already positive business case months before the pandemic began.

66. From a qualitive perspective, many intangible factors would have also supported EMV migration. The EDD beneficiaries were a highly vulnerable group, dependent upon their benefits to maintain their daily lives – making car payments, feeding families, and paying rent or mortgages – and that vulnerability would have only increased in the midst of a global pandemic.

67. Joseph's additional argument for why the Bank's decision not to issue EMV cards during the pandemic was reasonable raises a red herring. She argues that EMV would not "[h]ave [p]revented [a]ll the [r]eported [f]raud" and details, at length, first-party benefits and other possible types of fraud on the EDD portfolio, including fraud resulting from a lost or stolen card or phishing scheme or data breach. Joseph Rep. ¶¶51-57. But here, the only fraud relevant to the class is third-party, card-present counterfeit fraud. *See infra* ¶¶70-71. As detailed extensively in the Cloninger Report and below, EMV is highly effective at preventing card-present counterfeit fraud, specifically the type of card-present ATM transactions EDD customers reported. *See* Cloninger Rep. ¶¶29-45; *infra* ¶¶77-81.

68. Bank employees themselves concluded over and over again that EMV would have prevented much of the card-present counterfeit fraud on the EDD portfolio. In March of 2020, the Bank created a PowerPoint document to be presented to EDD that included talking points highlighting a "30% increase in impacted CA EDD cardholders submitting claims" year over year and stated that "67% of claims [in 2019] originate[d] from transactions made via channels that would be *directly curtailed by EMV (swiped, ATM)."*[27] Cloninger Report ¶¶ 72-73. In an email dated April 23, 2020, the Bank states, "Unfortunately, *fraudsters see our CA ATMs as a*

[27] BANA_EDD_MDL-167020 at -167022 (emphasis added).

jackpot source of vulnerable NON-chip cards,"[28]and in an email dated April 24, 2020, the Bank discusses the potential implications of fraud rings targeting Bank ATMS concluding "*if a fraudster put skimming devices on a CA ATM they would be getting a ton of CA EDD cards vulnerable because they are Mag only*."[29] And in a November 2020 email, "*as you know, the only way to stop counterfeit is EMV.*"[30] Cloninger Report ¶¶87-94.

69. Finally, Joseph misleadingly implies that EMV is ineffective because fraud claims continued after the Bank eventually converted to EMV. Joseph Rep. ¶¶74-75. Joseph cites Bank documents discussing only continued detection of first-party fraud to support this claim. However, as discussed below, only third-party, card-present counterfeit card transactions are at issue in this case – the specific transactions that EMV was designed to counter and has proven very effective at doing so.

D. EMV Would Have Prevented All or Nearly All of the Unauthorized ATM Withdrawals and Other Unauthorized Card-Present Transactions Class Members Experienced.

a. The Only Type of Fraud Relevant to this Class is Pin-Enabled, Card-Present Counterfeit Fraud, which EMV is Extremely Effective at Preventing.

70. Throughout the Joseph Report, Joseph discusses and includes in her various analyses many types of fraud and information compromise, including principally first-party benefits fraud, that are not relevant to this case. The only relevant fraud is card-present counterfeit card fraud, and more specifically unauthorized card-present ATM withdrawals done with a counterfeit card. EMV chips would have been extremely effective at preventing that type of fraud.

---

[28] BANA_EDD_MDL-297295 at -297295 (emphasis added).

[29] BANA_EDD_MDL-228914 at -228914 (emphasis added).

[30] BANA_EDD_MDL-163307 at -163307 (emphasis added).

71. The class definition in this lawsuit explicitly *excludes* individuals whom the Bank has determined engaged in benefits fraud or submitted fraudulent claims: "Excluded from each class is any person whom the Bank has determined, pursuant to its Remediation Plan with the United States Consumer Financial Protection Bureau (CFPB) and Office of the Comptroller of the Currency (OCC), [redacted] Mtn. for Class Cert at p.2. The class definition also only includes individuals who reported unauthorized transactions at an ATM, i.e., necessarily excludes people who only reported card-not-present transactions. Those transactions are thus not relevant to this class. Mtn. for Class Cert at p.1-2.

72. To the extent Joseph discusses types of fraud other than first-party benefits fraud, they are unlikely and unable to account for a significant amount of the unauthorized transactions at issue in this case.

73. 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. Joseph Rep. ¶¶16, 55, 56, 71, 86, 106, 126. 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.

74. First, fraud resulting from a lost or stolen card generally comprises a small percentage of overall reports of fraudulent transactions. A 2025 survey conducted by Security.org found that "[o]nly 8% of fraudulent charges involved stolen or lost credit cards," meaning the remaining 92% of fraudulent charges involved cards still in the owner's

possession.[31] 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 suggesting that such a unique factual scenario leading to fraud would comprise any significant portion of the unauthorized transactions class members experienced.

75. 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. 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. ¶100 n.71. 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%).[32] The survey does not discuss children using their parents' cards to make unauthorized ATM withdrawals.

76. The remainder of this part accordingly only discusses the efficacy of EMV at preventing card-present counterfeit, pin-enabled ATM transactions.

[31] Brett Cruz, 62 Million Americans Experienced Credit Card Fraud Last Year: 2025 Credit Card Fraud Report and Statistics, Security.org (Jan. 27, 2025), https://www.security.org/digital-safety/credit-card-fraud-report/.

[32] 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/.

b. EMV Chips are Highly Effective at Preventing Card-Present Counterfeit Fraud.

77. EMV is designed to make any stolen card data, including data stolen from [redacted] and/or card skimming/shimming, *useless* for completing a successful counterfeit card-present transaction. It is irrelevant that EMV technology does not prevent these forms of data theft; what matters is that EMV prevents such stolen data from being used to conduct counterfeit card transactions.

78. 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. For each EMV transaction, the chip in the card creates a unique, unpredictable code which is then encoded and can only be read by the issuer of that card. *See* Cloninger Rep. ¶¶29, 30, 45.

79. EMV chips are virtually impossible to clone because the chip never transmits the secret key stored inside it, a private key that can only be opened by the matching private key at the issuer which is also never transmitted.[33] *See* Cloninger Rep. ¶32. EMV does prevent the use of data from any source to be reused for card-present counterfeit transactions and specifically the ATM transactions at issue in this case. *See* Cloninger Rep. ¶¶33-34.

80. As EMV technology became widespread, use of EMV chips successfully and significantly reduced fraud around the world and was already showing significant reductions in fraud in the U.S. For example, in 2018 counterfeit card-present fraud in the UK was down by

[33] *See generally* EMV Key Management – Explained, CRYPTOMAThIC (2023), https://www.cryptomathic.com/hubfs/docs/cryptomathic_white_paper-emv_key_management.pdf.

90% compared to that reported in 2008,[34] in 2015, counterfeit card-present fraud was down by 92%[35] in Canada, and in 2019 the US was seeing 87%[36] declines in counterfeit card-present fraud at merchants who had converted to EMV. *See* Cloninger Rep. ¶44.

81. An increase in skimming incidents does not contradict this broad trend. Rather, any increase in skimming attacks demonstrates that criminals were trying to find mag-stripe only cards whose data could be successfully stolen *and used* to commit counterfeit card-present fraud.

c. To the Extent Any Counterfeit Fraud Could Have Nonetheless Succeeded on EMV Cards, the Scope Would Have Been Extremely Limited by Strict Fallback Rules in the Bank's Control.

82. Joseph focuses on the possibility of using counterfeit mag-stripe cards generated from cloned EMV ship cards at 1) non-chip enabled ATMs and POS and 2) at merchants or ATMs that allow mag-stripe transactions. This grossly overstates the risk from fallback transactions, which are transactions completed using the mag stripe of an EMV chip card rather than the chip card itself. *See* Cloninger Rep. ¶¶34-39. 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.

83. The first line of protection is the EMV chip card itself. When an EMV chip cardholder attempts to make a transaction at a chip-enabled terminal by swiping the mag-stripe

---

[34] Fraud the Facts 2019, UK Finance, 17 (2019), https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf.

[35] Jim Daly, With Its EMV Conversion Nearly Complete, Canada's POS Debit Fraud Falls to New Low (Feb. 25, 2016), https://www.digitaltransactions.net/with-its-emv-conversion-nearly-complete-canadas-pos-debit-fraud-falls-to-new-low/.

[36] Visa Chip Card Update, Visa (June 2019), https://usa.visa.com/content/dam/VCOM/blogs/visa-emvchip-infographicQ2-080819-v2a.pdf.

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 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 to process the transaction using that card.

84. If the ATM or POS terminal allows a fallback transaction to proceed, the ATM or POS terminal will typically send a code with the authorization request 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.[37] 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.

85. The next line of protection is the limits and fines placed on excessive fallback transactions by the card brands. Fallback transactions had been high during the initial years of EMV deployment, largely due to problems with implementation. Industry mitigation efforts include imposing transaction fees to penalize frequent fallback transactions. If fallback

[37] 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.

transactions at a given ATM exceed 2.5% for Visa or 3.0% for Mastercard, the networks impose penalty fees.[38] 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.

86. 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. Joseph also ignores that the Bank [redacted][9]

One Bank employee explained:

[redacted]

87. The Bank acknowledged [redacted][1] By 2021, one

[38] *Id.*

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

[40] *Id.*

[41] Ex. 164 at -57505.

[redacted]

[redacted][42]

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

89. The Bank's [redacted] The Bank experienced [redacted][43] 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.

d. Individual Inquiries Are Not Necessary to Determine if EMV Would Have Prevented Cardholders' Unauthorized Transactions.

90. Joseph contends multiple times that examination of individual circumstances for each transaction is necessary to know if the fraud was first-party fraud or, if not, if it could have been prevented by EMV. I disagree.

91. First, as discussed above, any individuals whom the Bank has determined engaged in first-party fraud are by definition excluded from the classes that Plaintiffs seek to

[42] Ex. 165 at -431012.

[43] 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.

certify. Second, 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. Because all class members are individuals who reported an unauthorized withdrawal from an ATM (necessarily a card-present transaction) and have not been determined by the Bank to have engaged in fraud, an EMV chip would have prevented the unauthorized ATM withdrawals that they reported.

92. Nevertheless, my understanding is that the Bank has in its records system details about each claim, including [redacted][44] 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][45] Again, the Bank could easily disaggregate those individuals from the people who [redacted].

93. To the extent Joseph details potential account takeovers resulting from the improper mailing of full account holder Social Security Numbers, *see* Joseph Rep. ¶¶85, 108, the

[44] *See* Ex. 166 at -205593 [redacted] -80·4 [redacted] · Ex. 167 at -001199 [redacted]

[45] *Id.*

Bank similarly tracked suspected fraud resulting from takeovers, as opposed to counterfeit fraud, and such individuals could be separated from the remainder of the class.[46]

IV. CONCLUSION

94. EMV was developed in the 1990s as a fraud prevention tool to counter the growing problem of card-present counterfeit fraud. It is globally recognized as the industry standard fraud protection for this category of fraud. The success of EMV technology is due to the unique code generated within the card's chip for each transaction. This code is never replicated and cannot be created without a legitimate EMV chip. EMV does not prevent card skimming or shimming or data loss through data breaches or phishing but does render that stolen data *useless* for making subsequent card-present transactions, thereby eliminating the value of the data for undertaking card-present counterfeit fraud attacks.

95. Nothing in the Joseph Report changes my opinion that EMV was the industry standard for the entire payments card industry by at least 2019, at which time a majority of the infrastructure was in place to support credit, debit and prepaid cards, including programs like EDD prepaid debit cards. Joseph mistakenly implies that the industry must be much more than majority, or 100%, converted for a standard to be in place. By 2019, industry data shows strong and growing participation in EMV among industry participants. Not only was the infrastructure in place but foreseeable shifts in the actions of fraudsters had already begun causing fraud rates to rise to unprecedented levels in segments of the industry that had previously been relatively unencumbered by fraud. EMV requires that all the interconnected programs and participants in the card payments industry participate to fight card-present counterfeit fraud. Any card issuer that has a Visa or MasterCard brand on it is incented by the liability shifts to use the EMV standard. The industry took great efforts to warn those portions of the industry who lagged in

[46] *See* BANA_EDD_MDL-00003038 at -3039.

migrating to EMV that they were vulnerable to significant losses, as happened with the Bank's EDD program and was foreseeable.

96. In concluding that the Bank acted reasonably in issuing mag-stripe only EDD cards before and during the pandemic, Joseph ignores that the Bank had a positive business case for moving EDD debit cards to EMV chips that Bank employees stated "ma[de] sense to move." *See supra* ¶64. In my professional experience, the Bank's decision to proceed without EMV chips in its EDD debit cards from January 2020 until July 2021, even after analyzing the costs and benefits of such a decision and determining the incremental cost of adding chips was only $0.39 per card and the Bank would recoup those costs by year two and gain net savings by year three, was highly irregular and not in line with what I would have expected from a highly sophisticated and well-resourced financial institution acting in good faith.

97. For all these reasons, nothing in the Joseph Report changes my opinion that any financial institution in the Bank's situation would have known or should have known that, due to Bank's decision to issue vulnerable mag-stripe only rather than EMV chip cards to its EDD debit cardholders prior to July 2021, many of its EDD debit cardholders who reported an unauthorized ATM withdrawal between April 1, 2020 and June 8, 2021 were in fact victims of card-present counterfeit fraud that likely resulted from card skimming. It is also my opinion that any financial institution in the Bank's situation would have known, and that the Bank did know or should have known, that its "Claim Fraud Filter" strategy would result in the wrongful denial of a substantial number of valid claims and the wrongful freezing of accounts of innocent EDD debit cardholders.

* * * * * *

Dated: April 4, 2025

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
3/19/21	Document		BANA_EDD_MDL-3038-46