

## **DX 12.A**

**REDACTED VERSION OF  
DOCUMENT SOUGHT TO  
BE SEALED PURSUANT TO  
STIPULATED  
PROTECTIVE ORDER**

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

IN RE: BANK OF AMERICA  
CALIFORNIA UNEMPLOYMENT  
BENEFITS LITIGATION

Case No. 1-MD-02992-GPC-MSB

**EXPERT REPORT OF PAMELA JOSEPH**

**March 4, 2025**

FILED PROVISIONALLY UNDER SEAL  
PURSUANT TO STIPULATED PROTECTIVE ORDER

## TABLE OF CONTENTS

|                                                                                                                                                                          |    |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----|
| I. QUALIFICATIONS .....                                                                                                                                                  | 3  |
| II. ASSIGNMENT.....                                                                                                                                                      | 4  |
| III. SUMMARY OF OPINIONS .....                                                                                                                                           | 5  |
| IV. BACKGROUND REGARDING EMV CHIP TECHNOLOGY .....                                                                                                                       | 7  |
| A. Magnetic Stripe (“Magstripe”) Card Technology .....                                                                                                                   | 7  |
| B. EMV Chip Technology .....                                                                                                                                             | 8  |
| C. Adoption of EMV Chip Technology in the U.S. Payment Card Industry.....                                                                                                | 8  |
| V. IT WAS REASONABLE FOR THE BANK TO ISSUE EDD PREPAID DEBIT CARDS WITHOUT EMV CHIPS.....                                                                                | 17 |
| A. EMV Chips Were Not Industry Standard for Prepaid Debit Cards .....                                                                                                    | 17 |
| B. It Was Reasonable for the Bank to Issue EDD Prepaid Debit Cards Without EMV Chips                                                                                     | 20 |
| C. Even With the Changes That Occurred During the Covid-19 Pandemic, It Remained Reasonable for the Bank to Issue EDD Prepaid Debit Cards Without EMV Chips .....        | 22 |
| VI. ADDING 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.....      | 28 |
| A. The Shifting of Liability for Fraud Does Not Eliminate Fraud.....                                                                                                     | 29 |
| B. EMV Chips Do Not Prevent All Fraud .....                                                                                                                              | 30 |
| C. EMV Chips Do Not Prevent Cards From Being Skimmed or Card Information From Otherwise Being Compromised .....                                                          | 32 |
| D. The Determination of Whether an EMV Chip Would Have Prevented Skimming or Other Information Compromise Requires Examination of Each Particular Incident of Compromise | 34 |
| E. Chips Would Not Have Prevented the Allegedly Unauthorized Transactions That Involved Fraud or Mistake by the Cardholder .....                                         | 35 |
| F. Chips Would Not Have Prevented All Fraudulent ATM Withdrawals Reported to the Bank Even if They Were Actually Unauthorized.....                                       | 38 |
| G. EMV Chips Would Not Have Prevented All Fraudulent Point-of-Sale Transactions.....                                                                                     | 42 |
| H. The Determination of Whether an EMV Chip Would Have Prevented a Particular Unauthorized Transaction Requires Examination of Each Transaction.....                     | 43 |
| VII. CONCLUSION.....                                                                                                                                                     | 44 |

## **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, and 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.

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”),<sup>1</sup> 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. I also reviewed the materials listed in the expert reports of Jane Cloninger in this matter dated August 29, 2024 (the “Cloninger Class Cert. Report”) and November 21, 2024 (the “Cloninger Class Cert. Rebuttal Report”).

## **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-referenced matter. I was asked to explain and provide background on magnetic stripe (“magstripe”) technology and Europay, Mastercard, and Visa (“EMV”) chip technology in connection with payment cards, and also to explain some of the factors relevant to decisions regarding card technology. I was further asked to provide my opinions on the following topics:

---

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

- a) The adoption of EMV chips in the payment card industry, particularly with respect to prepaid debit cards;
- b) Whether it was reasonable for the Bank to not convert the California Employment Development Department (“EDD”) prepaid debit cards (“EDD Prepaid Debit Cards”) to EMV chip technology prior to 2021;
- c) Whether EMV chips would have prevented card skimming, card shimming, or other unauthorized access to, or compromise of, cardholder information stored on a prepaid debit card; and
- d) Whether the addition of EMV chips to the EDD Prepaid Debit Cards issued by the Bank would have prevented the allegedly unauthorized transactions that were reported to the Bank on EDD Prepaid Debit Cards that did not have EMV chips.

### **III. SUMMARY OF OPINIONS**

13. The adoption of EMV chip technology for payment cards took place gradually and at different rates across different types of payment cards. Card issuers evaluated the characteristics of their specific card products and programs to determine whether and, if so, when it was warranted to convert a card product or program to EMV chip technology. There was no one-size-fits-all “payment card industry” adoption date or approach for the implementation of EMV chips. In particular, EMV chips were not standard for prepaid debit cards even after the 2015 change in payment card network rules, and were not standard in 2019 and 2020. In fact, of the in-person transactions made using general purpose prepaid debit cards in 2019, more than 74% of the

transactions and more than 75% of the dollar volume of such transactions were completed without a chip.<sup>2</sup>

14. It was reasonable for the Bank to have issued EDD Prepaid Debit Cards without EMV chips. The Bank's decision was supported by the characteristics of the EDD Prepaid Debit Card program, which included: i) the generally short-term or stop-gap nature of unemployment benefits; ii) the comparatively low balances of EDD Prepaid Debit Cards; and iii) the comparatively lower instances of observed fraud and amount of fraud losses.

15. Although reports of fraud increased during the Covid-19 pandemic, much of the fraud consisted of benefits fraud or other first-party fraud, which would not have been prevented by a conversion to chip cards. In addition, the logistics of converting EDD Prepaid Debit Cards to EMV technology would have disrupted the distribution of unemployment benefits to recipients during the expansion of the program in 2020. Finally, converting to EMV chip technology may not have been feasible due to the global chip shortage spurred on by the pandemic.

16. EMV chip technology does not prevent cards from being vulnerable to skimming, shimming, or other forms of information compromise. To that end, converting the EDD Prepaid Debit Cards issued by the Bank to EMV chip technology would not have prevented many of the unauthorized transactions that were reported to the Bank in 2020 and 2021. More specifically, EMV chips would not have prevented transactions that [REDACTED]

[REDACTED]

[REDACTED]

---

<sup>2</sup> Federal Reserve Payments Study, 2019. See Appendix C for percentage calculation. General purpose prepaid debit cards refer to network branded (*i.e.*, Visa, MasterCard, American Express, Discover), open-loop (*i.e.*, not restricted to a specific merchant) prepaid debit cards that share the same networks as non-prepaid debit cards). Almost 88% of these transactions occurred on reloadable cards, a feature shared with EDD cards.

[REDACTED]

[REDACTED]

[REDACTED]

17. 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 particular instance of alleged 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 specific transaction, including whether it was actually fraudulent, and where and how it was made.

#### **IV. BACKGROUND REGARDING EMV CHIP TECHNOLOGY**

##### **A. Magnetic Stripe (“Magstripe”) Card Technology**

18. Magstripe technology was introduced as a means of storing information on plastic cards by IBM in the early 1960s.<sup>3</sup> Within the banking and credit card industry, the technology became the most widespread mechanism for authorizing bank and credit card transactions and verifying identities over the course of the 1970s through the 1990s.<sup>4</sup>

19. Magstripe cards have a magnetic stripe on the back of the card that is made of iron particles in plastic film and which 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.

---

<sup>3</sup> “The magnetic stripe,” IBM, <https://www.ibm.com/history/magnetic-stripe> (Last visited on March 4, 2025).

<sup>4</sup> *Id.*

## **B. EMV Chip Technology**

20. EMV chip card technology was developed in the 1990s. EMV stands for “Europay, Mastercard and Visa,” the three companies that jointly helped to develop the EMV chip card standards in the 1990s. EMV chips store cardholder information on a metallic chip (in addition to the data that is stored on the card’s stripe). EMV chips create a single-use code when they are inserted into an EMV card reader to process a payment.<sup>5</sup> That code is different for each transaction made using the EMV chip, which can make it more difficult to make subsequent transactions using the code generated during a prior transaction.

21. Cards with EMV chips still feature magnetic stripes, which can also be used for payment. Although Mastercard has announced that it will start issuing cards without magnetic stripes in certain regions in the coming years, including Europe in 2024 and the U.S. in 2027, in 2020 and 2021 (and up to and including today), virtually all EMV chip cards issued in the U.S. still had a magnetic stripe in addition to a chip.<sup>6</sup>

## **C. Adoption of EMV Chip Technology in the U.S. Payment Card Industry**

22. Although EMV chip technology has been available since the 1990s, its usage only started to become more widespread for certain card products in the U.S. in the 2010s. The technology was not widely-adopted in the U.S. when it was introduced.<sup>7</sup>

---

<sup>5</sup> “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 March 4, 2025).

<sup>6</sup> “Swiping left on magnetic stripes”, MasterCard, August 12, 2021, <https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/> (Last visited on March 4, 2025).

<sup>7</sup> “The U.S. Migration to EMV: Considerations for the Payments Environment”, Federal Reserve Bank of Chicago – Payments Policy Group, May 18, 2015, [https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc\\_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7](https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7) (Last visited on March 4, 2025); “US EMV in 2013”, Alex Rolfe, February 3, 2014, <https://www.paymentscardsandmobile.com/us-emv-2013/#:~:text=On%20April%201%2C%202013%2C%20major%20card%20networks,%E2%80%9Cthe%20vast%20majority%20of%20US%20face%2Dto%2Dface%20sales> (Last visited on March 4, 2025).

## 1. Liability for Fraudulent Transactions

23. The major payment networks (*e.g.*, Visa and MasterCard, which provide the infrastructure and rules to facilitate debit and credit transactions) have rules to which merchants and card issuers using the networks must agree. These rules govern the transactions made on those networks, such as requirements for how transactions can or cannot be made, and certain processes that must be followed. Prior to October 2015, liability for fraudulent transactions was generally the responsibility of card issuers. Beginning in October 2015, the liability rules changed: as of that date, if a card has an EMV chip, but the merchant did not require the chip to be used in a fraudulent transaction, then the merchant is required to reimburse the card issuer for that transaction.<sup>8</sup>

24. The liability shift became effective in October 2015 and created financial incentives for both issuers and merchants with respect to the adoption of EMV chip technology in certain payment card products. Issuers were incentivized to review their portfolios of payment card products and programs to identify those that warranted incurring the expense and effort of migrating to EMV chip technology, in light of the change in cost-benefit considerations. Issuers generally took into account a variety of considerations, such as: i) the overall fraud exposure (*i.e.*, the potential liability for the issuer if cards were to be fraudulently compromised) in the program, including considerations such as average balances and the length of time funds were available on a card; ii) the potential for EMV chip technology to reduce the fraud risk (*i.e.*, whether EMV chips would prevent the types of fraud observed in the program); iii) the amount of fraud liability that could be shifted to merchants that did not adopt EMV chip technology; iv) the size of the program;

---

<sup>8</sup> Navigating the EMV Liability Shift, 2015, [https://fiscal.treasury.gov/files/cas/EMV\\_Liability\\_Customer\\_Toolkit\\_Vantiv.pdf](https://fiscal.treasury.gov/files/cas/EMV_Liability_Customer_Toolkit_Vantiv.pdf) (Last visited on March 4, 2025).

and v) the costs associated with migrating to EMV chip technology. The conversion to EMV chip technology for a particular card product or program typically required not only changes in card technology, design, and production, but also associated changes such as revisions to cardholder-facing documents and communications (*e.g.*, card mailers, websites, and cardholder agreements), updates to internal processes such as transaction monitoring and other fraud rules, and additional training for customer service representatives and other employees.

25. As issuers began converting certain card products and programs to EMV chip technology, merchants were incentivized to incur the optional cost of adding EMV chip-enabled terminals (ranging from \$200 to \$1,000 per terminal<sup>9</sup>), in order to potentially avoid incurring financial responsibility for fraudulent transactions.

26. The shift in card payment network liability rules was a primary catalyst for card issuers to implement EMV chip technology for certain card products and programs (to potentially shift to merchants the financial responsibility for fraudulent card-present transactions), and for merchants to install and use EMV chip terminals to process transactions (to potentially prevent that shift).

27. Notably, the change in card payment network rules in October 2015 did not include any requirement for card issuers to implement EMV chip technology or any requirement for merchants to install or use EMV chip terminals to process transactions. Indeed, a December 2015 Consumer Financial Protection Bureau (“CFPB”) report noted that implementing EMV technology is expensive for both issuers and merchants, that the transition to EVM technology

---

<sup>9</sup> The U.S. Migration to EMV: Considerations for the Payments Environment, Federal Reserve Bank of Chicago – Payments Policy Group, May 18, 2015, [https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc\\_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7](https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7) (Last visited on March 4, 2025).

may be confusing for consumers, and that merchants may be slow to adopt the technology.<sup>10</sup> The card payment networks have never adopted such a requirement. In fact, the network liability rules are structured to account for the fact that some issuers and merchants will use EMV technology and some will not, as the rules address the allocation of financial responsibility for non-EMV transactions.

28. As a result of all of these factors, adoption of EMV chips varied across the many different products that make up the “card industry.”

## **2. The Payment Card Industry Is a Collection of Diverse Products and Programs**

29. It is important to note that the “card industry” is not a single, homogenous collection of payment cards. Rather, there is wide variety in the type of products offered by card issuers, which, at a high level, can be categorized as including credit cards, debit cards, prepaid cards, and private-label cards. Each of these categories are described below, but it is also important to note that there are many different types of cards that fall within each category, as well as some products that do not fit neatly into any of these categories.

i) **Credit cards** provide the cardholder with access to a line of credit to make purchases, as well as cash advances. The cardholder is then obligated to pay at least some of the outstanding balance each billing cycle. There are myriad types of credit cards including standard credit cards, premium credit cards, affinity credit cards, co-branded credit cards, corporate credit cards, and cash secured credit cards, among others.

---

<sup>10</sup> CFPB, “The Consumer Credit Card Market”, December 2015, pp. 270-273, [https://files.consumerfinance.gov/f/201512\\_cfpb\\_report-the-consumer-credit-card-market.pdf](https://files.consumerfinance.gov/f/201512_cfpb_report-the-consumer-credit-card-market.pdf) (Last visited on March 4, 2025).

ii) **Debit cards** provide the cardholder with access to funds in their own checking or savings account at a bank (or credit union), which in turn can receive deposits from multiple sources (*e.g.*, direct deposit, checks, cash deposits, wire transfers from other accounts). When a purchase is made with a debit card, the amount of the transaction is withdrawn from the cardholder's checking or savings account. Generally, if a transaction is attempted for an amount greater than the balance of that account, the transaction will be declined. In some instances, subject to the terms of the applicable cardholder agreement(s), the bank may allow the transaction by extending an overdraft service or line of credit to the cardholder.

iii) **Prepaid debit cards** provide the cardholder with access to funds that have been pre-loaded onto the card. Prepaid debit cards are not linked to any checking or savings account and generally any account that is linked to a prepaid debit card can only receive funds from a single designated source. Prepaid debit cards generally do not provide access to a line of credit or overdraft service; the only funds that can be spent or withdrawn using a prepaid debit card are the funds that have previously been loaded onto the card. See Section V.A below for a further discussion of prepaid debit cards.

iv) **Private-label cards** include both private-label credit cards and private-label debit cards. They are generally issued by a retailer (*e.g.*, a department store chain or gas station chain) instead of a financial institution, can only be used only at that retailer and its affiliates, and generally do not use major payment networks like Visa or Mastercard.

### **3. Converting To EMV Chip Technology Was Generally a Product or Program Specific Decision for Issuers**

30. As described above, the October 2015 shift in card payment network rules changed the economic incentives surrounding the adoption of chip technology for certain payment card products. The economics, however, were not the same for every card product and program, as

different products and programs have vastly different profiles, characteristics, and risk exposure, which impacted the analysis of whether to implement a change to EMV chip technology.

31. Issuers would consider many factors when evaluating whether to convert a particular card product or program to EMV chip technology, such as: i) whether the card was linked to an underlying checking or savings account or line of credit and thus was a potential gateway to a larger store of funds; ii) the length of time funds were expected to be loaded and available through a card as longer time horizons presented greater potential fraud risk; and iii) the expected balance on the card where larger sums could involve higher fraud risk, as well as greater financial losses, among other considerations. Issuers also considered the expected usage patterns, such as whether cards in a particular program would be used abroad (*e.g.*, Europe) in places where EMV chip cards were far more prevalent. The assessment by issuers whether to implement EMV chip technology would vary for each product based on its unique characteristics.

32. In many instances, issuers made the business decision that converting to chip technology was not warranted for certain products, even after the change in card payment network rules in October 2015. Based on my 35 years of experience in the card and payments industry, there are a number of factors that supported a decision to not migrate a particular card product or program to EMV chip technology. These include the following:

i) **Card products or programs providing access to low balances** present comparatively lower fraud exposure for the issuer as the fraud loss is generally limited to the corresponding balance, and low-balance card products are generally less attractive of a target for fraudsters.

ii) **Card products or programs in which funds are generally available for only a short period of time** have comparatively less fraud exposure because they are less attractive

targets for fraudsters; thus, an issuer's potential responsibility for fraudulent transactions is also lower in these instances.

iii) **Card products or programs that are relatively modest in size** have comparatively less fraud exposure because they are less attractive targets for fraudsters; an issuer's potential responsibility for fraudulent transactions is also lower where the size of a program is smaller.

iv) **Card products or programs for which an issuer observes a relatively low incidence of card-present fraud** present comparatively less fraud exposure and responsibility for the issuer.

33. Because these types of considerations vary across different card products and programs, the change in card payment network rules in October 2015 did not result in adoption of EMV chips across all cards and all products. EMVCo, a consortium that develops and publishes EMV payment technology specifications and develops related testing processes, reported that in both 2020 and 2021—five years after the change in liability rules—37% of cards issued in the U.S. did not contain EMV chips.<sup>11</sup> Globally, 33% of cards in 2020 and 32% in 2021 did not have EMV chip technology.<sup>12</sup>

34. Notably, these figures reflect EMV chip adoption across *all* card products, covering various types of payment cards (including in the categories noted in Paragraph 29 above).

---

<sup>11</sup> EMVCo Worldwide EMV Deployment Statistics, <https://web.archive.org/web/20230126143112/https://www.emvco.com/about-us/worldwide-emv-deployment-statistics/> (Last visited on March 4, 2025)

<sup>12</sup> *Id.*

#### 4. Merchants Continue To Accept Magstripe Transactions

35. It is important to note that, in order for EMV chip-enabled cards to be used in chip-enabled transactions, merchants must have the infrastructure in place to leverage the EMV technology. Not surprisingly, the largest U.S. retailers were some of the first merchants to implement EMV payment terminals, while small and medium-sized businesses did not all immediately adopt the technology.<sup>13</sup> According to Visa, as of March 2017, the majority (56%) of merchant locations in the U.S. still did not accept EMV chip cards.<sup>14</sup> In March 2018, that percentage was 37%,<sup>15</sup> and in June 2019, almost four years after the liability shift in 2015, 20% of merchant locations in the U.S. still did not accept EMV chip cards.<sup>16</sup> In fact, [REDACTED]

[REDACTED]

[REDACTED]”<sup>17</sup>

36. Merchants that offer EMV chip readers also typically offer a card reader that reads magstripes as well. 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 also be used if the merchant does not require a chip.

---

<sup>13</sup> The U.S. Migration to EMV: Considerations for the Payments Environment, Federal Reserve Bank of Chicago – Payments Policy Group, May 18, 2015, [https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc\\_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7](https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transition-brief-051815-pdf.pdf?sc_lang=en&hash=A61CC6FAB897314421C31995EEB41FD7) (Last visited on March 4, 2025).

<sup>14</sup> Visa Chip Card Update: March 2017, <https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-emv-chip-infographic-mar-final.pdf> (Last visited on March 4, 2025).

<sup>15</sup> Visa Chip Card Update, March 2018, <https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-emv-chip-infographic-q1-2018.pdf> (Last visited on March 4, 2025).

<sup>16</sup> Visa Chip Card Update, June 2019, <https://usa.visa.com/content/dam/VCOM/blogs/visa-emvchip-infographicQ2-080819-v2a.pdf> (Last visited on March 4, 2025).

<sup>17</sup> [REDACTED]  
BANA\_EDD\_MDL-00198287-BANA\_EDD\_MDL-00198289, at BANA\_EDD\_MDL-00198289.

37. Additionally, EMV chips on cards can be scratched or damaged (*e.g.*, through excessive heat/water) or become dirty and 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 to 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.

38. 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 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). Issuers may set rules for such situations as well. For instance, after EDD agreed to allow the Bank to convert the EDD Prepaid Debit Card program to EMV chip technology in 2021,<sup>18</sup> [REDACTED]

[REDACTED]  
[REDACTED].<sup>19</sup>

39. Further, when a card (whether it has an EMV chip or not) 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.

---

<sup>18</sup> Executed letter from D. Haddock, Sr. Client Manager, March 17, 2021, BANA\_EDD\_MDL-00002230-BANA\_EDD\_MDL-00002231, at BANA\_EDD\_MDL-00002230.

<sup>19</sup> Document [REDACTED] BANA\_EDD\_MDL-00505808.

**V. IT WAS REASONABLE FOR THE BANK TO ISSUE EDD PREPAID DEBIT CARDS WITHOUT EMV CHIPS**

40. Based on my 35 years of experience in the card and payments industry, given the profile and characteristics of the EDD Prepaid Debit Cards and related industry practice, it was reasonable for the Bank to issue EDD Prepaid Debit Cards that did not have EMV chip technology.

41. I also note that the Bank needed EDD's approval to convert to EMV chip technology in 2021.<sup>20</sup> EDD did not provide its approval prior to March 17, 2021.

**A. EMV Chips Were Not Industry Standard for Prepaid Debit Cards**

42. Although some products were converted to EMV chip technology shortly before or after the 2015 change in network liability rules, EMV chips were not industry standard for prepaid debit cards, principally because of their distinctly lower-risk characteristics.

43. Prepaid debit cards as a product generally have lower fraud exposure than other payment cards, particularly consumer debit and credit cards. This is because:

i) **Prepaid debit cards have lower balances and fewer available funds** – In my experience, prepaid debit cards generally have lower balances and fewer available funds than many other card products including standard consumer debit cards or credit cards.

ii) **Prepaid debit cards are not tied to a consumer checking or savings account or line of credit** - Prepaid debit cards generally only provide access to the funds loaded onto the card. By contrast, consumer debit cards can provide access to an underlying checking or savings account where the cardholder often accumulates funds from various sources over time, along with an overdraft line of credit, and consumer credit cards have a line of credit;

---

<sup>20</sup> Executed letter from D. Haddock, Sr. Client Manager, March 17, 2021, BANA\_EDD\_MDL-00002230-BANA\_EDD\_MDL-00002231, at BANA\_EDD\_MDL-00002230.

all of those funds are potentially exposed to fraud. Also, many prepaid debit card programs are shorter in duration due to the nature of the programs and funds are only expected to be loaded and available for a limited period of time.

44. For prepaid debit cards, fraud exposure is limited to the amount of prepaid funds on the card, which is generally significantly lower than the accumulated funds in a checking or savings account. The lack of access to an overdraft or traditional line of credit, and the limited duration of many pre-paid debit card programs, further limit the amount and risk of fraud exposure. Accordingly, issuers were exposed to less risk of financial responsibility for fraudulent transactions, and generally did not convert prepaid debit cards to EMV technology following the liability shift in 2015. Cardholders were also exposed to lower risk of loss given the lower balances on these cards.

45. The continued prevalence of magstripe-only prepaid debit cards is reflected in Federal Reserve data concerning in-person transactions, which reflect that even in 2019, more than 74% of in-person transactions using general purpose prepaid debit cards were completed without a chip.<sup>21</sup> See Appendix C. In 2020, more than 65% of transactions with general purpose prepaid cards were completed without a chip, and 2021, nearly 54% transactions were made without a chip.<sup>22</sup>

46. Similarly, Federal Reserve data show that in 2019, approximately 75.8% of the dollar volume of in-person transactions using general purpose prepaid cards were completed

---

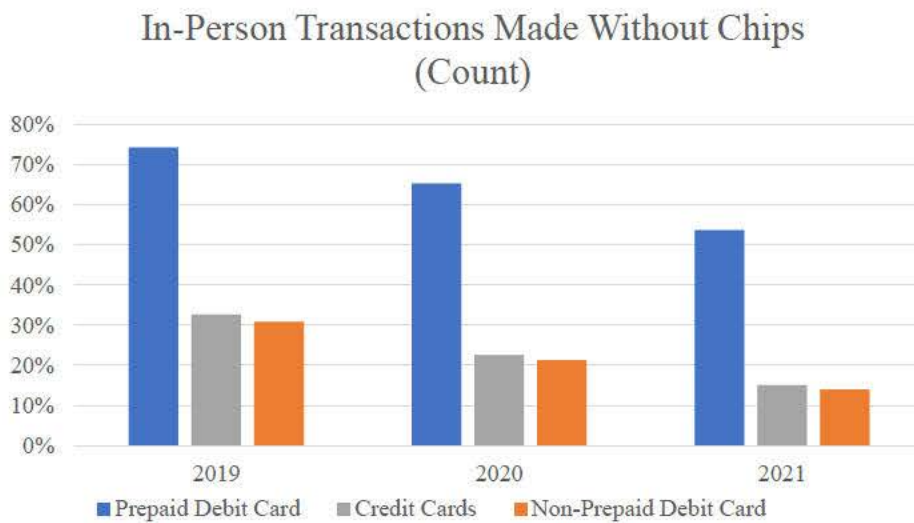
<sup>21</sup> Federal Reserve Payments Study, 2019. See Appendix C for percentage calculation. General purpose prepaid debit cards refer to network branded (*i.e.*, Visa, MasterCard, American Express, Discover), open-loop (*i.e.*, not restricted to a specific merchant) prepaid debit cards that share the same networks as non-prepaid debit cards). Almost 88% of these transactions occurred on reloadable cards, a feature shared with EDD cards.

<sup>22</sup> Federal Reserve Payments Study, 2022. See Appendix C for percentage calculation.

without a chip.<sup>23</sup> In 2020 and 2021, the proportional dollar volumes of in-person transactions using general purpose prepaid cards that were completed without a chip were approximately 68.3% and 57.2%, respectively.<sup>24</sup>

47. In comparison, in the years 2019 to 2021, for *non*-prepaid debit cards, only approximately 30.8%, 21.2%, and 14.0% of in-person transactions were completed without a chip.<sup>25</sup> Over the same period for credit cards, only approximately 32.7%, 22.5%, and 15.0% of in-person transactions were completed without a chip.<sup>26</sup> As noted above, the corresponding figures for prepaid debit cards were 74.4%, 65.5%, and 53.7%. See Figure 1.

Figure 1



<sup>23</sup> Federal Reserve Payments Study, 2022. See Appendix C for percentage calculation.

<sup>24</sup> Federal Reserve Payments Study, 2022. See Appendix C for percentage calculation.

<sup>25</sup> Federal Reserve Payments Study, 2022. See Appendix C for percentage calculation.

<sup>26</sup> Federal Reserve Payments Study, 2022. See Appendix C for percentage calculation.

**B. It Was Reasonable for the Bank to Issue EDD Prepaid Debit Cards Without EMV Chips**

48. There were several features of the EDD Prepaid Debit Card program, particularly prior to the onset of the Covid-19 pandemic in March 2020, that made it reasonable for the Bank to continue issuing EDD Prepaid Debit Cards without EMV chips:

i) **EDD Prepaid Debit Cards had low balances.** EDD unemployment insurance benefits are the single source of funding for the cards; no other funds can be added.<sup>27</sup> Prior to the pandemic, qualified beneficiaries could receive between \$40 and \$450 per week; the maximum weekly benefit was \$450 even for the highest earners and benefits were available for up to 26 weeks for a maximum of \$11,700 (\$450 x 26 weeks).<sup>28</sup> In 2019, recipients received on average of \$330 per week.<sup>29</sup> Consistent with the limited amount of funding for the cards, average card balances were relatively low prior to the pandemic. [REDACTED]

[REDACTED].<sup>30</sup> Based on my 35 years of experience in the card and payments industry, such low card balances generally make prepaid card products less attractive to fraudsters.

ii) **EDD Prepaid Debit Cards are a short-term program.** EDD Prepaid Debit Cards are issued for the single purpose of distributing unemployment insurance benefits, which by the nature of the program are stop gap or short-term benefits. Prior to the pandemic,

---

<sup>27</sup> EDD Debit Card Account Agreement, effective March 1, 2018, BANA\_EDD\_MDL-00536398-BANA\_EDD\_MDL-00536406, at BANA\_EDD\_MDL-00536398.

<sup>28</sup> See For Your Benefit: California's Programs for the Unemployed, pp. 4-5, [https://edd.ca.gov/siteassets/files/pdf\\_pub\\_ctr/de2320.pdf](https://edd.ca.gov/siteassets/files/pdf_pub_ctr/de2320.pdf) (Last visited on March 4, 2025).

<sup>29</sup> Unemployment Insurance for Workers Impacted by COVID-19, Legislative Analyst's Office, updated March 16, 2021, <https://lao.ca.gov/Publications/Report/4208> (Last visited on March 4, 2025).

<sup>30</sup> Bank EDD Prepaid Debit Card data, BANA\_EDD\_MDL-00884199.

recipients only received benefits so long as they remained unemployed and eligible, and only up to a maximum of 26 weeks.<sup>31</sup> To remain eligible, beneficiaries were required to re-certify every two weeks, be physically able and available to work, be looking for work each week, and be ready and willing to accept work right away.<sup>32</sup> If a benefits recipient starts a new job, loses eligibility, or exhausts the maximum weeks of available benefits, the benefits are terminated and no more funds are loaded to the beneficiaries' EDD Prepaid Debit Cards.<sup>33</sup> In 2019, beneficiaries under the EDD program received benefits for an average of 17 weeks.<sup>34</sup> Accordingly, card balances generally remained low, as the program is designed to be temporary in nature and funds are only expected to be loaded and available for a limited period of time, making the cards less attractive to fraudsters.

iii) **The size of the EDD program was relatively modest prior to the pandemic.** The number of cards issued for new EDD accounts per month was relatively small and had actually declined prior to the pandemic. Smaller card programs have less fraud risk, as described above, because fraudsters are less likely to target the programs and the cards are less likely to be caught up in broader fraud schemes due to the limited number of cards in use. Smaller programs also present lower exposure for issuers. [REDACTED]

---

<sup>31</sup> Unemployment Insurance for Workers Impacted by COVID-19, Legislative Analyst's Office, updated March 16, 2021, <https://lao.ca.gov/Publications/Report/4208> (Last visited on March 4, 2025). During the pandemic, benefits extensions were available through different programs that allowed some beneficiaries to receive benefits for as long as 99 weeks.

<sup>32</sup> See California Unemployment Eligibility Requirements, <https://edd.ca.gov/en/unemployment/eligibility/> (Last visited on March 4, 2025).

<sup>33</sup> *Id.*

<sup>34</sup> Unemployment Insurance for Workers Impacted by COVID-19, Legislative Analyst's Office, updated March 16, 2021, <https://lao.ca.gov/Publications/Report/4208> (Last visited on March 4, 2025).

[REDACTED]

[REDACTED]<sup>35</sup>

iv) **EDD Prepaid Debit Cards were generally not a target for fraud prior to the pandemic.** [REDACTED]

[REDACTED]

[REDACTED]<sup>36</sup>

49. For all of these reasons, it was reasonable for the Bank to issue EDD Prepaid Debit Cards without EMV chips. Issuing EDD Prepaid Debit Cards without EMV chips was also consistent with industry practice at the time (see Section V.A above).

**C. Even With the Changes That Occurred During the Covid-19 Pandemic, It Remained Reasonable for the Bank to Issue EDD Prepaid Debit Cards Without EMV Chips**

50. Soon after the onset of the Covid-19 pandemic, the EDD program experienced significant growth. In the months that followed, the Bank became aware of various types of fraudulent activity taking place. However, it remained reasonable for the Bank not to convert the EDD Prepaid Debit Cards to EMV technology.

**1. EMV Chips Would Not Have Prevented All the Reported Fraud**

51. [REDACTED]

[REDACTED]<sup>37</sup> The volume

---

<sup>35</sup> Bank EDD Prepaid Debit Card data, BANA\_EDD\_MDL-00884198.

<sup>36</sup> [REDACTED]  
[REDACTED]  
[REDACTED] Bank EDD Prepaid Debit Card data, BANA\_EDD\_MDL-00884199, and BANA\_EDD\_MDL-00884200.

<sup>37</sup> See Bradley Garfield deposition, December 10, 2024, 164:20 – 166:21; 167:21 – 168:15.

of EDD benefits fraud that took place in 2020 is staggering. The California State Auditor sent a letter to the Governor and Legislative Leaders in California stating:

EDD did not take substantive action to bolster its fraud detection efforts for its UI [unemployment insurance] program until months into the pandemic, resulting in payments of about \$10.4 billion for claims that it has since determined may be fraudulent because it cannot verify the claimants' identities. Specifically, EDD waited about four months to automate a key anti-fraud measure, took incomplete action against claims filed from suspicious addresses, and removed a key safeguard against improper payments without fully understanding the significance of the safeguard.<sup>38</sup>

52. An internal Bank of America document similarly notes that [REDACTED]

[REDACTED] ”<sup>39</sup> 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).<sup>40</sup> To add further perspective, a U.S. Government Accountability Office report dated September 2023 estimated that the fraud in the U.S. Department of Labor's unemployment insurance program during the pandemic—from April 2020 through May 2023 – was likely between \$100 billion and \$135 billion.<sup>41</sup>

53. Internal Bank communications show [REDACTED]

---

<sup>38</sup> Declaration of Laura Brys in Support of Defendant's Opposition to Plaintiffs' Motion for Class Certification, Ex. (“DX”) 88, CA State Auditor, “Weaknesses in EDD's Approach,” January 2021, BANA\_EDD\_MDL-00080294-BANA\_EDD\_MDL-00080352, at BANA\_EDD\_MDL-00080296.

<sup>39</sup> DX 112, EDD Validation Protocol – BofA GFC Questions, February 12, 2021, BANA\_EDD\_MDL-00073529-BANA\_EDD\_MDL-00073531, at BANA\_EDD\_MDL-00073530.

<sup>40</sup> DX 11, “David Manoucheri, “Analysis shows California EDD fraud at \$32.6 billion and counting,” KCRA3, October 6, 2022, <https://www.kcra.com/article/analysis-edd-fraud-326-billion-and-counting/41281662> (Last visited on March 4, 2025).

<sup>41</sup> GAO, Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely Between \$100 Billion and \$135 Billion, GAO-23-106696 (Washington, D.C.: Sept. 12, 2023), <https://www.gao.gov/products/gao-23-106696> (Last visited on March 4, 2025).

[REDACTED].<sup>42</sup> In some instances, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>43</sup> In fact, [REDACTED]

[REDACTED].<sup>44</sup>

54. None of that first-party fraud would have been prevented by EMV chips. It was therefore reasonable for the Bank to not respond immediately to these increased reports of fraud by migrating to EMV chip technology.

55. [REDACTED]

[REDACTED].<sup>45</sup> In such instances, EMV chips would similarly have no effect on preventing fraud.

56. Moreover, as discussed in more detail below, to the extent some of the unauthorized transactions reported to the Bank concerned actual fraud against the cardholder, EMV chip cards would not have prevented many of those transactions. For example, the presence of an EMV chip would not have prevented the use of a lost or stolen card. It also would not have prevented fraud committed using information compromised in ways that an EMV chip could not have prevented, e.g., a phishing scheme or merchant hack.

57. Thus, even though the number of fraud claims increased at the beginning of the Covid-19 pandemic, it was reasonable to continue issuing magstripe-only cards. Indeed, further

---

<sup>42</sup> Email from B. Garfield re [REDACTED], September 15, 2020, BANA\_EDD\_MDL-00706295-BANA\_EDD\_MDL-00706303, at BANA\_EDD\_MDL-00706296.

<sup>43</sup> See Bradley Garfield deposition, December 10, 2024, 164:21 – 168:5.

<sup>44</sup> Email from R. Schwartz re [REDACTED], September 24, 2020, BANA\_EDD\_MDL-00293490-BANA\_EDD\_MDL-00293492, at BANA\_EDD\_MDL-00293490-91.

<sup>45</sup> See Bradley Garfield deposition, December 10, 2024, 166:3-15.

confirming that EMV chips would not have prevented all of the fraud that was reported to the Bank, [REDACTED]

[REDACTED]<sup>46</sup>

## **2. The Pandemic Created Unprecedented Challenges for The Implementation of EMV Chip Technology**

58. There are additional reasons why it was reasonable to not immediately convert the EDD Prepaid Debit Card program to EMV chip technology at the beginning of the Covid-19 pandemic.

59. The challenges presented by Covid-19 made it unreasonable to attempt a rollout of EMV chip technology in the first year of the pandemic. These challenges included the sudden expansion of the program, as well as global supply chain issues.

60. Prior to the pandemic, the number of new EDD accounts each month was fairly stable. [REDACTED]<sup>47</sup>

[REDACTED]  
[REDACTED]  
[REDACTED]<sup>48</sup> [REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]<sup>49</sup> Among other things, [REDACTED]  
[REDACTED]

---

<sup>46</sup> Email from W. Martin re Increasing claims trend, August 31, 2021, BANA\_EDD\_MDL-00654305-BANA\_EDD\_MDL-00654307, at BANA\_EDD\_MDL-00654306.

<sup>47</sup> Bank EDD Prepaid Debit Card data, BANA\_EDD\_MDL-00884198.

<sup>48</sup> *Id.*

<sup>49</sup> Email from F. Ahmad re CA EDD Update, March 27, 2020, BANA\_EDD\_MDL-00102964-BANA\_EDD\_MDL-00102966, at BANA\_EDD\_MDL-00102964.

[REDACTED]

[REDACTED].<sup>50</sup> Moreover, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].<sup>51</sup>

61. Had EDD approved and allowed the Bank to attempt to begin converting EDD Prepaid Debit Cards to EMV chip technology at that time, it would have inevitably led to delays in card issuance, thus disrupting the Bank's efforts to issue cards to EDD cardholders. Implementing chip technology into a product like the EDD Prepaid Debit Cards is not a task that can be completed overnight, and can take months, as it is a complex and multi-faceted process requiring several elements, including materials sourcing, design and production of the chipped cards, design and production of new card package materials to educate cardholders, changes to fraud tools, and developing and implementing training for Bank employees (including call center agents) to assist in managing the inevitable disruption the migration will cause for card holders.

[REDACTED]

[REDACTED]<sup>52</sup> In addition, in this instance, the Bank needed EDD's approval to convert to EMV chip technology, which took several months of discussions in 2021.<sup>53</sup> [REDACTED]

---

<sup>50</sup> *Id.*; Email from B. Garfield re Daily Prepaid Cards Update 4/8/22020, April 9, 2020, BANA\_EDD\_MDL-00130068-BANA\_EDD\_MDL-00130069.

<sup>51</sup> Email from F. Ahmad re CA EDD Update, March 27, 2020, BANA\_EDD\_MDL-00102964-BANA\_EDD\_MDL-00102966, at BANA\_EDD\_MDL-00102964-65.

<sup>52</sup> Email from B. Garfield re EMV 1 pager, December 23, 2020, BANA\_EDD\_MDL-00405089.

<sup>53</sup> See William Martin deposition, February 14, 2024, 114:4 – 114:7; Executed letter from D. Haddock, Sr. Client Manager, March 17, 2021, BANA\_EDD\_MDL-00002230-BANA\_EDD\_MDL-00002231, at BANA\_EDD\_MDL-00002230; Document "Bank of America and California EDD Weekly Meeting", February 5,

[REDACTED]

[REDACTED].<sup>54</sup>

62. Given the amount of time that it would have taken to implement chip technology in 2020, and the many challenges that the Bank was facing as a result of the pandemic, the Bank's focus on getting cards to cardholders so that they would have access to their funds, rather than prioritizing a migration to chips that would have delayed the distribution of unemployment benefits to cardholders, was reasonable.

63. Moreover, because of the disruption wrought by the pandemic, particularly to supply chains, there was a global chip shortage that would have further hindered the Bank's ability to implement chip technology in EDD Prepaid Debit Cards.<sup>55</sup> Attempting to add chips to the cards in the throes of the pandemic, during the unprecedented expansion of the EDD program, and in the midst of a global chip shortage would have caused even more disruption to the issuance and distribution of EDD Prepaid Debit Cards.

---

2021, BANA\_EDD\_MDL-00253674-BANA\_EDD\_MDL-00253676, at BANA\_EDD\_MDL-00253674; Email from C. Webb re [REDACTED], BANA\_EDD\_MDL-00447117-BANA\_EDD\_MDL-00447118.

<sup>54</sup> Email from C. Webb re [REDACTED], BANA\_EDD\_MDL-00447117- BANA\_EDD\_MDL-00447118.

<sup>55</sup> The semiconductor shortage has been described as due to a "perfect storm" of factors. Prior to 2020, there were already difficulties in obtaining inputs for production, including semiconductor manufacturing equipment used to make older varieties of chips, and components used in electronic assembly such as diodes, capacitors, and substrates. There was also an underlying growth in demand for chips as industries shifted to more semiconductor-intensive products (e.g., electric vehicles, 5G). The pandemic exacerbated these trends by dramatically increasing demand for products that require semiconductors of all types. Simultaneously, supply was disrupted by a series of black swan events such as factory fires, winter storms, energy shortages, and COVID-19-related shutdowns. "Results from Semiconductor Supply Chain Request for Information", U.S. Department of Commerce, January 20, 2022, <https://www.commerce.gov/news/blog/2022/01/results-semiconductor-supply-chain-request-information> (Last visited on March 4, 2025). See also Global chip shortage threatens payment card supply," American Banker, Kate Fitzgerald, May 27, 2021, <https://www.americanbanker.com/payments/news/global-chip-shortage-threatens-payment-card-supply> (Last visited on March 4, 2025).

64. As noted above, in March 2021 the Bank and EDD signed an agreement for the implementation of EMV chip technology.<sup>56</sup> The distribution of chip cards then began in July 2021.<sup>57</sup> Considering the characteristics of the EDD Prepaid Debit Cards, the unprecedented challenges of the global pandemic, and the complexity of the migration to chip cards discussed above, the actual timeline by which the Bank implemented chips into the EDD Prepaid Debit Cards was reasonable.

**VI. ADDING 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**

65. In addition to failing to prevent skimming and other forms of compromise, EMV chip cards (1) do not prevent many instances of actual or alleged fraud and (2) would not have prevented all of the unauthorized transactions reported to the Bank. 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 alleged compromise occurred and how each alleged unauthorized transaction was made.

a) Based on my experience overseeing and running a card-issuing business, EMV chip technology would not have prevented all of the fraud reported to the Bank in 2020 and 2021, including all card-present counterfeit fraud for the Bank's EDD prepaid debit cardholders at chip-enabled ATMs and POS terminals.

b) There are 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,

---

<sup>56</sup> See William Martin deposition, February 14, 2024, 114:4 – 114:7; Executed letter from D. Haddock, Sr. Client Manager, March 17, 2021, BANA\_EDD\_MDL-00002230-, BANA\_EDD\_MDL-00002231.

<sup>57</sup> See William Martin deposition, February 14, 2024, 65:4 – 65:7.

phishing, or other means, and EMV chip cards can still be stolen. EMV chips also do not prevent all ATM fraud.

c) 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.

66. 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 U.S., any assumption that EMV chip technology would prevent all fraud for card-present transactions, including ATM fraud, is at odds with the reality experienced in the industry during this time and with the nature of card fraud and how it occurs.

#### **A. The Shifting of Liability for Fraud Does Not Eliminate Fraud**

67. 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.

68. As discussed above, under the liability-shift rules that took effect in October 2015, the liability (*i.e.*, financial responsibility) for a fraudulent transaction rested with the party (card issuer or merchant) that did not offer EMV technology. 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 transaction from occurring but may have prevented the card issuer from bearing financial liability for the loss.

69. I address below whether EMV chips would have prevented the transactions that were reported to the Bank as fraudulent, irrespective of whether the use of EMV chip technology would have allowed the Bank to shift financial responsibility for those losses.

**B. EMV Chips Do Not Prevent All Fraud**

70. 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 EMV chips on EDD Prepaid Debit Cards would have prevented all or even most of the fraud reported to the Bank in 2020 and 2021.

71. 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, in determining whether EMV chips would have prevented an allegedly unauthorized transaction, one must consider whether the reported transaction was actually fraudulent, or whether it reflected cardholder fraud or mistake.

72. Second, as discussed further below, EMV chips do not prevent fraud when the reportedly unauthorized transactions involve instances where the cardholder claims that their card was lost or stolen, or never received (*e.g.*, it was stolen in the mail). In each of those instances,

the EMV chip would not prevent the criminal in possession of the lost or stolen card from using the card in the same way the cardholder could, including at an ATM, or for point-of-sale or other transactions. Thus, one must consider whether the cardholder was still in possession of their card, or whether the alleged fraudster had possession.

73. Third, even as to third-party fraud actually experienced by cardholders who maintained possession of their cards (which cannot be identified without the assessment described above), EMV chips still would not have prevented all of these transactions. 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.

74. Indeed, card fraud has continued to increase, notwithstanding the presence of EMV chips on cards. A December 2020 Nilson Report, a periodical specific to the card industry, quantified annual global card-fraud losses at \$23.97 billion in 2017, which then increased 20 percent to \$28.65 billion by 2019.<sup>58</sup> 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.<sup>59</sup>

75. 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, and

---

<sup>58</sup> Nilson Report, Issue 1187, December 2020, Page 1.

<sup>59</sup> FICO Blog, August 16, 2022. <https://www.fico.com/blogs/us-card-skimming-fraud-grows-700-first-half-2022> (Last visited on March 4, 2025).

- c) The generation of random numbers until a legitimate account is stumbled upon.

**C. EMV Chips Do Not Prevent Cards From Being Skimmed or Card Information From Otherwise Being Compromised**

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

[REDACTED]

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

78. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

79. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

80. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED] 60

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

83. Beyond skimmers, there are also “shimmers,” which are thin devices that can be

[REDACTED]

[REDACTED] 61

[REDACTED]

84. 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;<sup>62</sup> thus, PIN compromises typically do not result from skimming but occur in other ways that are not prevented by the use of EMV chip technology.

85. Chips also do not prevent other forms of information compromise (*e.g.*, phishing, merchant data breaches, other security attacks). EMV chip data can be captured from point-of-sale terminals, and EMV-Bypass Cloning was recognized as a problem by July 2020.<sup>63</sup> The December 2020 Nilson Report described 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

---

<sup>60</sup> DX 41, Email re [REDACTED], BANA\_EDD\_MDL-00164188; DX 42, ATM Data re Ex. 41, October 24, 2020, BANA\_EDD\_MDL-00164189.

<sup>61</sup> “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 on March 4, 2025) 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](https://www.wqow.com/news/shimmers-the-new-credit-card-skimmers/article_8a075616-886b-558d-9a42-8ca5ea3e578f.html) (Last visited on March 4, 2025).

<sup>62</sup> “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 on March 4, 2025).

<sup>63</sup> “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 on March 4, 2025).

value of annual sales of PII in the \$1 billion range.<sup>64</sup> [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED].<sup>65</sup> 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 prevented any of these compromises.

86. Finally, as noted above, the presence of EMV chips do not prevent physical theft or loss of the card itself, nor do they prevent a criminal or fraudster from engaging in unauthorized transactions using a lost or stolen card.

**D. The Determination of Whether an EMV Chip Would Have Prevented Skimming or Other Information Compromise Requires Examination of Each Particular Incident of Compromise**

87. Therefore, 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 information compromise.

88. In order to determine whether an EMV chip would have prevented skimming, one has to consider the circumstances surrounding the usage of the card at the time it was skimmed

[REDACTED]

[REDACTED]

[REDACTED]

89. For example, [REDACTED]

[REDACTED]

---

<sup>64</sup> Nilson Report, Issue 1187, December 2020, Page 5.

<sup>65</sup> DX 17, Letter from Elaine M. Howle, November 19, 2020, BANA\_EDD\_MDL-00422774-BANA\_EDD\_MDL-00422779, at BANA\_EDD\_MDL-00422776.

[REDACTED]

90. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

91. One must also consider the behavior of the merchant, including whether the merchant [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

92. For all these reasons, one must look at the circumstances surrounding a particular compromise to assess whether it could have been avoided through the addition of an EMV chip.

**E. Chips Would Not Have Prevented the Allegedly Unauthorized Transactions That Involved Fraud or Mistake by the Cardholder**

93. Further, any assumption that all fraud reported to Bank of America was, in fact, fraud actually targeting the cardholder, is both unfounded and implausible. One would have to review each report to determine whether the cardholder actually experienced third-party fraud, or whether the cardholder is committing first-party fraud or made a mistaken report.

94. First, EMV chips do not prevent individuals from committing benefits fraud. Based on review of the materials in this case, 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.

95. The California State Auditor found that EDD paid “about \$10.4 billion for claims that it has since determined may be fraudulent because it cannot verify the claimants’ identities.”<sup>66</sup>

[REDACTED]

[REDACTED]

[REDACTED]<sup>67</sup> 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).<sup>68</sup>

96. 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, as chips do not prevent fraudsters from using the chip cards that they obtain through fraud.

97. Second, cardholders may also falsely report that a transaction was fraudulent; EMV chips cannot prevent these transactions. This includes both cardholders who obtained their cards and accounts fraudulently, as described above, and 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

---

<sup>66</sup> DX 88, CA State Auditor, “Weaknesses in EDD’s Approach,” January 2021, BANA\_EDD\_MDL-00080294-BANA\_EDD\_MDL-00080352, at BANA\_EDD\_MDL-00080296.

<sup>67</sup> DX 112, [REDACTED], BANA\_EDD\_MDL-00073529-BANA\_EDD\_MDL-00073531, at BANA\_EDD\_MDL-00073530.

<sup>68</sup> DX 11, “David Manoucheri, “Analysis shows California EDD fraud at \$32.6 billion and counting,” KCRA3, October 6, 2022, <https://www.kcra.com/article/analysis-edd-fraud-326-billion-and-counting/41281662> (Last visited on March 4, 2025).

a target for individuals who make 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 and merchants” and “[a]ll of these loss estimates originate at a single point: when the consumer disputes a transaction.”<sup>69</sup>

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]<sup>70</sup> EMV chips would not have prevented (and did not prevent) this type of fraud.

99. 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 which are falsely reported as fraudulent, regardless of who the cardholder is.

100. 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 may not realize that another authorized user of their card (*e.g.*, a family member) was responsible

---

<sup>69</sup> “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 on March 4, 2025).

<sup>70</sup> DX 113, Email from B. Welch re Prepaid Dark Web, November 3, 2021, BANA\_EDD\_MDL-00151781-BANA\_EDD\_MDL-00151783, at BANA\_EDD\_MDL-00151781.

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.<sup>71</sup> Socure reports that 29% of Americans who committed first-party fraud say that it was an accident.<sup>72</sup> 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.

101. 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 may be a result of fraud and/or mistake, as described above.

**F. Chips Would Not Have Prevented All Fraudulent ATM Withdrawals Reported to the Bank Even if They Were Actually Unauthorized**

102. EMV chips would not have prevented all fraudulent ATM transactions even if they were determined to be actually unauthorized.

103. First, 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, which would require a PIN compromise in addition to the skimming/cloning of the card. Although pinhole cameras and keypad overlays are devices that can be used to capture a PIN, they are separate from skimmers

---

<sup>71</sup> “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 March 4, 2025).

<sup>72</sup> “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 on March 4, 2025).

and the skimming of a card does not necessarily involve a PIN compromise as well, and EMV chips do not prevent these methods of PIN compromise.

104. Further, in the case of any cloned or counterfeit cards made using [REDACTED] [REDACTED] an EMV chip card would not have prevented that compromise.

105. Second, for any reported unauthorized transactions to the Bank involving cards that the cardholder claimed were physically stolen or lost, adding an EMV chip would not have prevented the 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.

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

107. To this point, a September 2015 Experian survey 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.”<sup>73</sup> 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

---

<sup>73</sup> Experian Press Release, January 28, 2016. <https://www.experianplc.com/newsroom/press-releases/2016/data-privacy-day-survey> (Last visited on March 4, 2025).

whether banks prohibit weak PINs such as 1234.”<sup>74</sup> 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,” and that 41% have compromised their PIN security in other ways, [REDACTED]

[REDACTED]<sup>75</sup>

108. In addition, the EDD program itself could have exposed cardholders to potential fraudulent activity. As noted above, EDD sent 51 million pieces of mail with information that could be used for identity theft or to access existing accounts.<sup>76</sup> As reflected in [REDACTED]

[REDACTED]<sup>77</sup> [REDACTED]

[REDACTED] EMV chips cannot prevent this type of fraud.

109. Third, EMV chips would not have prevented transactions using information that was compromised in a manner other than skimming or shimming, as in instances where a cardholder reports that they never used their card, or never used it for a point-of-sale or ATM transaction, before the allegedly unauthorized transaction. If the card was not skimmed or

---

<sup>74</sup> “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](https://www.cl.cam.ac.uk/~rja14/Papers/BPA12-FC-banking_pin_security.pdf) (Last visited on March 4, 2025).

<sup>75</sup> RBC Press Release, March 9, 2020. <https://www.rbc.com/newsroom/news/article.html?article=125249> (Last visited on March 4, 2025).

<sup>76</sup> DX 17, BANA\_EDD\_MDL-00422774-BANA\_EDD\_MDL-00422779, at BANA\_EDD\_MDL-00422774-BANA\_EDD\_MDL-00422775.

<sup>77</sup> DX 115, Email from F. Ahmad re Updates on CA EDD accounts, December 9, 2020, BANA\_EDD\_MDL-00061630-BANA\_EDD\_MDL-00061632, at BANA\_EDD\_MDL-00061632.

shimmed, the EMV chip would not have prevented the compromise of that information, and that compromised information could still be used in a number of ways.

110. Fourth, EMV chips would not prevent fraud from occurring on non-chip enabled 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,<sup>78</sup> meaning that 7% of U.S. ATMs still did not require chips. These non-chip-enabled ATMs rely [REDACTED]

[REDACTED]

[REDACTED]

111. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

112. 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.”<sup>79</sup> Likewise, [REDACTED]

[REDACTED]

[REDACTED]

80

---

<sup>78</sup> VISA U.S. EMV Migration Summary, June 2020, BANA\_EDD\_MDL-00292669-BANA\_EDD\_MDL-00292675, at BANA\_EDD\_MDL-00292673.

<sup>79</sup> FICO Blog, March 6, 2024. <https://www.fico.com/blogs/debit-card-compromises-nearly-doubled-2023-fico-data> (Last visited on March 4, 2025).

<sup>80</sup> DX 114, Email from S. Daniels re CTF Swiped as % of Total, April 29, 2021, BANA\_EDD\_MDL-00118617-BANA\_EDD\_MDL-00118618, at BANA\_EDD\_MDL-00118617.

113. [REDACTED]

[REDACTED]

[REDACTED]

114. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

81

115. For all of these reasons, one cannot simply conclude that the presence of an EMV chip would have prevented all fraudulent ATM transactions. One would need to consider many factors, such as the ATM used or available, and the circumstances surrounding compromise of the card or card information. Each of these determinations must be made by looking at the circumstances surrounding each unique transaction.

**G. EMV Chips Would Not Have Prevented All Fraudulent Point-of-Sale Transactions**

116. EMV chips also would not have prevented all of the fraudulent point-of-sale transactions reported to the Bank, including those using a physical card (card-present transactions) as well as those that do not require use of a physical card (card-not-present transactions).

117. Chips provide no protection to [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

81

”, BANA\_EDD\_MDL-00505808.

[REDACTED]

[REDACTED] Adding an EMV chip does not stop this process.

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

[REDACTED] 82

[REDACTED] 83

**H. The Determination of Whether an EMV Chip Would Have Prevented a Particular Unauthorized Transaction Requires Examination of Each Transaction**

119. 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.

120. One would have to first consider whether the transaction was actually fraudulent, or whether it reflects an instance of cardholder fraud or mistake.

121. 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,

---

<sup>82</sup> Bank of America and California EDD Weekly Meeting, Meeting Notes, February 5, 2021, BANA\_EDD\_MDL-00198287-BANA\_EDD\_MDL-00198289, at BANA\_EDD\_MDL-00198289.

<sup>83</sup> “EMV Bypass Cloning,” Chargebacks911, February 2, 2023, <https://chargebacks911.com/emv-bypass-cloning/> (Last visited on March 4, 2025).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

122. 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]

[REDACTED]

[REDACTED]

[REDACTED]

## VII. CONCLUSION

123. The adoption of EMV chip technology for payment cards took place gradually and at different times across the different types of payment cards. Card issuers evaluated the characteristics of their specific card products and programs to determine whether and, if so, when it was warranted to convert a card product or program to EMV chip technology. There was no one-size-fits-all “payment card industry” adoption date for the addition of EMV chips to all cards, as there is no uniform “payment card industry.” Although some card products and programs adopted EMV chips around the time of, or soon after, the 2015 change in payment card network rules, other card products and programs did not generally adopt EMV chips until several years later. For prepaid debit cards, in particular, EMV chips were not standard for a number of years, including in 2019 and 2020; in fact, more than 74% of in-person transactions with general purpose prepaid cards and more than 75% of the dollar volume of those transactions in 2019 were made without a chip.

124. It was reasonable for the Bank to have issued EDD Prepaid Debit Cards without EMV chips. This was supported by the characteristics of the program prior to the Covid-19 pandemic, which presented less fraud exposure compared to other types of payment card products.

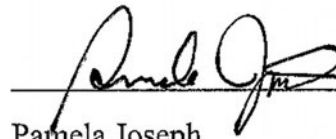
125. It was reasonable for the Bank to continue to issue magstripe-only cards during the Covid-19 pandemic. Much of the fraud that was reported to the Bank during the pandemic was of a nature that could not have been prevented by EMV chips (including benefits fraud and other first-party fraud). Further, the undertaking of converting EDD Prepaid Debit Cards to EMV technology would have disrupted the distribution of unemployment benefits to recipients during the dramatic expansion of the program in 2020. And converting all EDD Prepaid Debit Cards in 2020 may not have been feasible due to the global chip shortage spurred on by the pandemic.

126. EMV chip technology also does not prevent cards from being vulnerable to skimming, shimming, or other forms of information compromise. To that end, EMV chip technology would not have prevented many of the alleged unauthorized transactions that were reported to the Bank in 2020 and 2021, including transactions that were not third-party fraud, as well as various instances of third-party fraud (*e.g.*, involving non-chip-enabled terminals or lost or stolen cards) and card-not-present transactions.

127. 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 particular instance of 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.

CONFIDENTIAL

Executed this 4<sup>th</sup> day of March 2025



Pamela Joseph

**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

*In RE Bank of America California Unemployment Benefits Litigation*

**Expert Report 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 Rebuttal Report of Jane Cloninger in Support of Plaintiffs' Motion for Class Certification dated November 21, 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

Defendant's Memorandum of Points and Authorities in Opposition to Plaintiffs' Motion for Class Certification dated October 24, 2024

Plaintiff's Reply in Support of Motion for Class Certification dated November 21, 2024

**3. Depositions and Exhibits**

William Matt Martin Deposition Transcript

Michael Letson Deposition Transcript

Shane Daniels Deposition Transcript

Faiz Ahmad Deposition Transcript

Bradley Garfield Deposition Transcript

**4. Other Produced Documents**

BANA\_EDD\_MDL-00002230-BANA\_EDD\_MDL-00002231

BANA\_EDD\_MDL-00057504-BANA\_EDD\_MDL-00057506

BANA\_EDD\_MDL-00059312-BANA\_EDD\_MDL-00059315

BANA\_EDD\_MDL-00059316-BANA\_EDD\_MDL-00059318

BANA\_EDD\_MDL-00061630-BANA\_EDD\_MDL-00061632

BANA\_EDD\_MDL-00073529-BANA\_EDD\_MDL-00073531

BANA\_EDD\_MDL-00074993-BANA\_EDD\_MDL-00075000

BANA\_EDD\_MDL-00080294-BANA\_EDD\_MDL-00080352

BANA\_EDD\_MDL-00102964-BANA\_EDD\_MDL-00102966

BANA\_EDD\_MDL-00104742-BANA\_EDD\_MDL-00104746

BANA\_EDD\_MDL-00116001-BANA\_EDD\_MDL-00116002

BANA\_EDD\_MDL-00116003-BANA\_EDD\_MDL-00116005

BANA\_EDD\_MDL-00117094-BANA\_EDD\_MDL-00117096

BANA\_EDD\_MDL-00118617-BANA\_EDD\_MDL-00118618

BANA\_EDD\_MDL-00123235-BANA\_EDD\_MDL-00123236

BANA\_EDD\_MDL-00130068-BANA\_EDD\_MDL-00130069

BANA\_EDD\_MDL-00151781-BANA\_EDD\_MDL-00151783

BANA\_EDD\_MDL-00163307-BANA\_EDD\_MDL-00163308

BANA\_EDD\_MDL-00164188

BANA\_EDD\_MDL-00164189

BANA\_EDD\_MDL-00164190

BANA\_EDD\_MDL-00167020-BANA\_EDD\_MDL-00167024

BANA\_EDD\_MDL-00172469-BANA\_EDD\_MDL-00172473

BANA\_EDD\_MDL-00198287-BANA\_EDD\_MDL-00198289

BANA\_EDD\_MDL-00253674-BANA\_EDD\_MDL-00253676

BANA\_EDD\_MDL-00292669-BANA\_EDD\_MDL-00292675

BANA\_EDD\_MDL-00292991-BANA\_EDD\_MDL-00292992

BANA\_EDD\_MDL-00293490-BANA\_EDD\_MDL-00293492

BANA\_EDD\_MDL-00351839-BANA\_EDD\_MDL-00351840

BANA\_EDD\_MDL-00352396-BANA\_EDD\_MDL-00352397

BANA\_EDD\_MDL-00356089-BANA\_EDD\_MDL-00356095

BANA\_EDD\_MDL-00358713-BANA\_EDD\_MDL-00358718

BANA\_EDD\_MDL-00370150-BANA\_EDD\_MDL-00370155

BANA\_EDD\_MDL-00401305-BANA\_EDD\_MDL-00401312

BANA\_EDD\_MDL-00405089

BANA\_EDD\_MDL-00422774-BANA\_EDD\_MDL-00422779

BANA\_EDD\_MDL-00447117-BANA\_EDD\_MDL-00447118

BANA\_EDD\_MDL-00455617-BANA\_EDD\_MDL-00455619

BANA\_EDD\_MDL-00505808

BANA\_EDD\_MDL-00536398-BANA\_EDD\_MDL-00536406

BANA\_EDD\_MDL-00624545-BANA\_EDD\_MDL-00624547

BANA\_EDD\_MDL-00654305-BANA\_EDD\_MDL-00654307

BANA\_EDD\_MDL-00706295-BANA\_EDD\_MDL-00706303

BANA\_EDD\_MDL-00881813-BANA\_EDD\_MDL-00881814

BANA\_EDD\_MDL-00884198

BANA\_EDD\_MDL-00884199

BANA\_EDD\_MDL-00884200

## 5. Publicly Available Documents

Alex Rolfe, "US EMV in 2013," February 3, 2014, available at <https://www.paymentscardsandmobile.com/us-emv-2013/#:~:text=On%20April%201%2C%202013%2C%20major%20card%20networks,%E2%80%9Cthe%20vast%20majority%20of%20US%20face%2Dto%2Dface%20sales>

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>

Bureau of the Fiscal Service, "Navigating the EMV Liability Shift," Vantiv, 2015, available at [fiscal.treasury.gov/files/cas/EMV\\_Liability\\_Customer\\_Toolkit\\_Vantiv.pdf](https://fiscal.treasury.gov/files/cas/EMV_Liability_Customer_Toolkit_Vantiv.pdf)

Business Wire, "Bank of America Begins Rollout of Chip Debit Cards," September 30, 2014, available at [www.businesswire.com/news/home/20140930005292/en/Bank-of-America-Begins-Rollout-of-Chip-Debit-Cards](https://www.businesswire.com/news/home/20140930005292/en/Bank-of-America-Begins-Rollout-of-Chip-Debit-Cards)

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](https://www.cl.cam.ac.uk/~rja14/Papers/BPA12-FC-banking_pin_security.pdf)

CFPB, "The Consumer Credit Card Market," December 2015, available at [https://files.consumerfinance.gov/f/201512\\_cfpb\\_report-the-consumer-credit-card-market.pdf](https://files.consumerfinance.gov/f/201512_cfpb_report-the-consumer-credit-card-market.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>

Employment Development Department, “California Unemployment Benefit Programs,” updated August 2021, available at [edd.ca.gov/siteassets/files/unemployment/pdf/benefit-flowchart.pdf](http://edd.ca.gov/siteassets/files/unemployment/pdf/benefit-flowchart.pdf)

Employment Development Department, “For Your Benefit: California’s Programs for the Unemployed,” updated January 2024, available at [https://edd.ca.gov/siteassets/files/pdf\\_pub\\_ctr/de2320.pdf](https://edd.ca.gov/siteassets/files/pdf_pub_ctr/de2320.pdf)

Employment Development Department, “Unemployment Eligibility Requirements,” available at <https://edd.ca.gov/en/unemployment/eligibility/>

Employment Development Department, “Unemployment Insurance Benefit Table for New Claims with a Beginning Date of January 2, 2005 or After,” available at [https://edd.ca.gov/siteassets/files/pdf\\_pub\\_ctr/de1101bt5.pdf](https://edd.ca.gov/siteassets/files/pdf_pub_ctr/de1101bt5.pdf)

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, Internet Archive, “Worldwide EMV® Deployment Statistics,” 2023, available at <https://web.archive.org/web/20230126143112/https://www.emvco.com/about-us/worldwide-emv-deployment-statistics/>

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>

EMVCo, “Worldwide EMV® Deployment Statistics,” 2024, available at [www.emvco.com/about-us/worldwide-emv-deployment-statistics/](https://www.emvco.com/about-us/worldwide-emv-deployment-statistics/)

EMV Migration Forum, “Near-Term Solutions to Address the Growing Threat of Card-Not-Present Fraud,” Version 2.0, July 2016, available at [www.emv-connection.com/downloads/2015/04/CNP-Solutions-White-Paper-Version-2-FINAL-July-2016.pdf](http://www.emv-connection.com/downloads/2015/04/CNP-Solutions-White-Paper-Version-2-FINAL-July-2016.pdf)

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>

Federal Reserve Payments Study, 2016

Federal Reserve Payments Study, 2019

Federal Reserve Payments Study, 2022

Federal Reserve Payments Study Glossary, Survey Period: Calendar Year 2022

Federal Reserve Payments Study Networks, Processors, and Issuers Payments Survey (NPIPS) Data, 2015-2022

FinCen Advisory, “Advisory on Unemployment Insurance Fraud during the Coronavirus Disease 2019 (COVID-19) Pandemic,” October 13, 2020, available at [www.fincen.gov/sites/default/files/advisory/2020-10-13/Advisory%20Unemployment%20Insurance%20COVID%2019%20508%20Final.pdf](http://www.fincen.gov/sites/default/files/advisory/2020-10-13/Advisory%20Unemployment%20Insurance%20COVID%2019%20508%20Final.pdf)

Kate Fitzgerald, American Banker, “Global Chip Shortage Threatens Payment Card Supply,” May 26, 2021, available at [www.americanbanker.com/payments/news/global-chip-shortage-threatens-payment-card-supply](http://www.americanbanker.com/payments/news/global-chip-shortage-threatens-payment-card-supply)

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>

Kandice Alter and Anna Neumann, Federal Reserve Bank of Chicago, “The U.S. Migration to EMV: Considerations for the Payments Environment,” May 18, 2015, available at <https://www.chicagofed.org/-/media/others/markets/payments-policy/emv-transitionbrief-051815pdf.pdf?sclang=en&hash=A61CC6FAB897314421C31995EEB41FD7>

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>

Legislative Analyst's Office, "Unemployment Insurance for Workers Impacted by COVID-19," updated March 16, 2021, available at [lao.ca.gov/Publications/Report/4208](http://lao.ca.gov/Publications/Report/4208)

Nilson Report, Issue 1187, December 2020

Nilson Report, Issue 1252, November 2022

Rashmi Ramesh, Bank Info Security, "Stripping the Magnetic Stripe: What's Taking so Long?" July 6, 2023, available at [www.bankinfosecurity.com/stripping-magnetic-stripe-whats-taking-so-long-a-22461](http://www.bankinfosecurity.com/stripping-magnetic-stripe-whats-taking-so-long-a-22461)

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://www.socure.com/resources/reports/solving-the-elusive-challenge-of-first-party-fraud>

Tracy Scott, WQOW, "Shimmers: the new credit card skimmers," June 29, 2018, available at [https://www.wqow.com/news/shimmers-the-new-credit-card-skimmers/article\\_8a075616-886b-558d-9a42-8ca5ea3e578f.html](https://www.wqow.com/news/shimmers-the-new-credit-card-skimmers/article_8a075616-886b-558d-9a42-8ca5ea3e578f.html)

U.S. Department of Commerce, "Results from Semiconductor Supply Chain Request for Information," January 2025, 2022, available at [www.commerce.gov/news/blog/2022/01/results-semiconductor-supply-chain-request-information](http://www.commerce.gov/news/blog/2022/01/results-semiconductor-supply-chain-request-information)

U. S. Government Accountability Office, "Unemployment Insurance: Estimated Amount of Fraud during Pandemic Likely between \$100 Billion and \$135," September 13, 2023, available at [www.gao.gov/products/gao-23-106696](http://www.gao.gov/products/gao-23-106696)

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

Visa, "Visa Chip Card Update," March 2017, available at <https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-emv-chip-infographic-mar-final.pdf>

Visa, "Visa Chip Card Update," March 2018, available at <https://usa.visa.com/dam/VCOM/global/visa-everywhere/documents/visa-emv-chip-infographic-q1-2018.pdf>

CONFIDENTIAL

Visa, "Visa Chip Card Update," June 2019, available at  
<https://usa.visa.com/content/dam/VCOM/blogs/visa-emvchip-infographicQ2-080819-v2a.pdf>

Note: I also reviewed the materials listed in Appendix B of the Expert Class Certification Report of Jane Cloninger dated August 29, 2024 and Appendix B of the Rebuttal Class Certification Report of Jane Cloninger dated November 21, 2024.

*In RE Bank of America California Unemployment Benefits Litigation***General Purpose Payment Cards: In-Person Transactions Without Chips****2019 - 2021**

(Transaction Count in Billions)

**Prepaid Debit Cards<sup>[a]</sup>**

|             | [A]             | [B]   | [C]   | [D]   |
|-------------|-----------------|-------|-------|-------|
|             | Category        | 2019  | 2020  | 2021  |
| (1)         | Total In-Person | 4.9   | 5.8   | 5.9   |
| (2)         | Chip            | 1.2   | 2.0   | 2.7   |
| (3)         | No Chip         | 3.6   | 3.8   | 3.2   |
| (4)=(3)/(1) | % No Chip       | 74.4% | 65.5% | 53.7% |

**Non-Prepaid Debit Cards<sup>[b]</sup>**

|             | [A]             | [B]   | [C]   | [D]   |
|-------------|-----------------|-------|-------|-------|
|             | Category        | 2019  | 2020  | 2021  |
| (5)         | Total In-Person | 58.3  | 52.4  | 59.0  |
| (6)         | Chip            | 40.3  | 41.2  | 50.8  |
| (7)         | No Chip         | 18.0  | 11.1  | 8.2   |
| (8)=(7)/(5) | % No Chip       | 30.8% | 21.2% | 14.0% |

**Credit Cards<sup>[c]</sup>**

|               | [A]             | [B]   | [C]   | [D]   |
|---------------|-----------------|-------|-------|-------|
|               | Category        | 2019  | 2020  | 2021  |
| (9)           | Total In-Person | 28.0  | 21.2  | 26.9  |
| (10)          | Chip            | 18.8  | 16.5  | 22.9  |
| (11)          | No Chip         | 9.1   | 4.8   | 4.0   |
| (12)=(11)/(9) | % No Chip       | 32.7% | 22.5% | 15.0% |

*Totals may not sum due to rounding.*Source: Federal Reserve Payment Study, 2022.

*In RE Bank of America California Unemployment Benefits Litigation***General Purpose Payment Cards: In-Person Transactions Without Chips****2019 - 2021**

(Transaction Value in \$ Trillions)

**Prepaid Debit Cards<sup>[a]</sup>**

|             | [A]             | [B]   | [C]   | [D]   |
|-------------|-----------------|-------|-------|-------|
|             | Category        | 2019  | 2020  | 2021  |
| (1)         | Total In-Person | 0.13  | 0.19  | 0.23  |
| (2)         | Chip            | 0.03  | 0.06  | 0.10  |
| (3)         | No Chip         | 0.10  | 0.13  | 0.13  |
| (4)=(3)/(1) | % No Chip       | 75.8% | 68.3% | 57.2% |

**Non-Prepaid Debit Cards<sup>[b]</sup>**

|             | [A]             | [B]   | [C]   | [D]   |
|-------------|-----------------|-------|-------|-------|
|             | Category        | 2019  | 2020  | 2021  |
| (5)         | Total In-Person | 1.78  | 1.76  | 2.16  |
| (6)         | Chip            | 1.34  | 1.48  | 1.92  |
| (7)         | No Chip         | 0.44  | 0.28  | 0.25  |
| (8)=(7)/(5) | % No Chip       | 24.8% | 15.9% | 11.4% |

**Credit Cards<sup>[c]</sup>**

|               | [A]             | [B]   | [C]   | [D]   |
|---------------|-----------------|-------|-------|-------|
|               | Category        | 2019  | 2020  | 2021  |
| (9)           | Total In-Person | 1.60  | 1.25  | 1.73  |
| (10)          | Chip            | 1.15  | 1.02  | 1.41  |
| (11)          | No Chip         | 0.45  | 0.23  | 0.32  |
| (12)=(11)/(9) | % No Chip       | 28.3% | 18.1% | 18.5% |

*Totals may not sum due to rounding.*Source: Federal Reserve Payment Study, 2022.

*In RE Bank of America California Unemployment Benefits Litigation*

**General Purpose Payment Cards: In-Person Transactions Without Chips 2019 – 2021**

**Notes:**

[a] Per the Federal Reserve’s Depository and Financial Institutions Payments Survey (DFIPS) for the survey period of calendar year 2022, survey recipients who issued general-purpose prepaid cards received the below instruction regarding the reporting of general-purpose prepaid card program accounts.

Prepaid card transactions are the portion of debit card transactions associated with prepaid debit card accounts, which accounts include “accounts for both reloadable and non-reloadable open-loop prepaid cards for which your institution was the issuer. Your customer may or may not be able to add additional funds to this card after it has been issued and use these funds to shop, transfer money, or pay bills...

Include:

- General-purpose prepaid card programs managed by both your institution and a third-party
- Individual and pooled general-purpose prepaid card program accounts for which your institution is the issuer...
- Consumer and business/government general-purpose open-loop reloadable prepaid card program accounts
- Consumer and business/government general-purpose open-loop non-reloadable prepaid card program accounts
- Open-loop gift card accounts
- Payroll prepaid card program accounts
- FSA/HAS medical card accounts
- Government-administered general-purpose open-loop prepaid card program accounts
- Customer refund and incentive card accounts
- Consumer and business/government general-purpose prepaid card program accounts for which only virtual cards are issued (no physical card)

Do not include:

- Closed-loop prepaid card program accounts (i.e., prepaid cards that don’t route transactions over a debit card network)

**Appendix C.3**  
Confidential

- Debit card accounts
- ATM or ATM-only accounts
- Electronic benefits transfer (EBT) card accounts
- Credit card accounts”<sup>1</sup>

[b] Per the Federal Reserve’s Depository and Financial Institutions Payments Survey (DFIPS) for the survey period of calendar year 2022, survey recipients who issued general-purpose non-prepaid debit cards received the below instruction regarding the reporting of general-purpose non-prepaid debit card program accounts.

Includes “all transactions made with debit cards via any debit card network (details below) and associated with non-prepaid accounts held by your institution... Most debit cards are capable of being processed through a dual-message network as well as one or more single-message networks. Includes cash-back transactions at the point of sale but does not include cash withdrawals (typically from an automated teller machine (ATM) or over the counter at a bank branch). Transactions may originate at a physical point of sale or remotely such as via mail order, telephone order, or online, such as through e-commerce or bill pay sites via an app or web browser. For this study, please follow these guidelines:

[Non-prepaid] Debit card transactions include...

- Transactions made with Visa, MasterCard, Discover, or American Express branded cards and cleared over dual-message networks. These are typically called signature-based or offline debit card transactions.
- Transactions made with debit cards and cleared over a general-purpose single-message network. Transactions originated in other countries with debit cards issued from U.S. domiciled accounts
- Debit card cash-back transactions at the point of sale

[Non-prepaid] Debit card transactions do not include...

- ATM withdrawals
- Credit card transactions
- Prepaid card transactions
- Transfers by a corporate customer to fund its employees' payroll card accounts

---

<sup>1</sup> The Federal Reserve Payments Study Glossary Survey Period: Calendar Year 2022, pp 4, 39.

- Electronic Benefits Transfer (EBT) card transactions made using a proprietary network (e.g., Quest network) for that purpose
- Payroll card transactions by the cardholder”<sup>2</sup>

[c] Per the Federal Reserve’s Depository and Financial Institutions Payments Survey (DFIPS) for the survey period of calendar year 2022, survey recipients who issued general-purpose credit cards received the below instruction regarding the reporting of general-purpose credit card program accounts.

All transactions over any credit card network made with general-purpose credit cards, charge cards or co-branded credit cards issued by your institution including “general-purpose credit card accounts for which your institution was the issuer...

Include:

- All general-purpose credit card accounts, including zero-balance active accounts, with a credit line and the ability to transact
- Accounts for general-purpose credit cards your institution issues on behalf of another institution
- Virtual general-purpose credit card accounts

Do not include:

- Any credit card accounts for which your institution was not the card issuing institution
- Private-label credit or charge card accounts whose cards can only be used at a limited set of merchants and that do not use one of the four major credit card networks
- Debit or prepaid card program accounts
- Transaction deposit accounts
- Closed accounts”<sup>3</sup>

---

<sup>2</sup> The Federal Reserve Payments Study Glossary Survey Period: Calendar Year 2022, pp 38-39.

<sup>3</sup> The Federal Reserve Payments Study Glossary Survey Period: Calendar Year 2022, pp 7, 53.