

PX 2

CONTAINS CONFIDENTIAL MATERIAL

**UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF CALIFORNIA**

IN RE BANK OF AMERICA CALIFORNIA
UNEMPLOYMENT BENEFITS
LITIGATION

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

EXPERT REPORT OF JANE CLONINGER

March 4, 2025

REDACTED PUBLIC VERSION

CONTAINS CONFIDENTIAL MATERIAL

TABLE OF CONTENTS

I. ASSIGNMENT	1
II. SUMMARY OF EXPERT QUALIFICATIONS.....	2
III. HOURLY RATE	4
IV. FACTS AND DATA CONSIDERED.....	4
V. SUMMARY OF OPINIONS	5
VI. STATEMENT OF OPINIONS AND BASIS FOR OPINIONS	7
A. Mag-Stripe Only Cards Are Highly Vulnerable to Skimming and Card-Present Counterfeit Fraud	7
B. EMV Chips Are Extremely Effective at Preventing Card-Present Counterfeit Fraud.....	14
C. By At Least 2019, EMV Chips Were the Industry Standard for Credit and Debit Card Security.....	21
D. The Bank’s Failure to Include EMV Chips in its EDD Debit Cards Resulted in Cards with Below Industry Standard Security	28
E. The Bank’s Decision to Not Include EMV Chips in EDD Debit Cards in Early 2020 Was Inconsistent with Other Participants in the Payments Industry	29
F. It Was Highly Foreseeable that the Bank’s Failure to Include EMV Chips in EDD Debit Cards Would Lead to Counterfeit Fraud Targeting EDD Debit Cardholders During the Pandemic, Because Fraud Migrates to the Weakest Link	38
G. The Bank’s Decision Not to Issue EMV Chip Cards to EDD Debit Cardholders Led to an Increase in Skimming Attacks Targeting California EDD Cards.....	44
H. EMV Chip Cards Would Have Prevented All or Nearly All of the Unauthorized ATM Withdrawals and Other Unauthorized Card-Present Transactions Class Members Experienced	46
I. Any Financial Institution in the Bank’s Situation Would Have Known that Many EDD Cardholders Who Reported Unauthorized PIN-Enabled ATM Withdrawals Were True Victims of Counterfeit Fraud	49
VII. CONCLUSION	52

CONTAINS CONFIDENTIAL MATERIAL

I. ASSIGNMENT

1. I have been retained as an expert in this matter by co-lead counsel for Plaintiffs, Cotchett, Pitre & McCarthy, LLP and Altshuler Berzon LLP (collectively, “Plaintiffs’ Counsel”).

2. Plaintiffs’ Counsel have informed me that from 2011 to approximately February 15, 2024, the Bank had an exclusive contract with California’s Employment Development Department (“EDD”) to distribute unemployment insurance (“UI”), disability insurance, and paid family leave benefits to Californians through Bank-issued prepaid debit cards (“EDD debit cards”).¹ Prior to July 2021, all EDD debit cards were “mag-stripe only” debit cards that did not contain an “EMV” chip (terms explained below).²

3. Plaintiffs’ Counsel asked me to provide my expert opinion with respect to certain issues relevant to this litigation, including but not limited to:

- a. Whether Bank of America’s (the “Bank’s”) failure to embed EMV chips in its EDD debit cards between March 2020 and June 2021 was consistent with industry standards for debit card security;
- b. Whether the Bank’s failure to include EMV chips in its EDD debit cards between March 2020 and June 2021 foreseeably rendered those cards vulnerable to card skimming attacks and card-present counterfeit card fraud, including unauthorized withdrawals at Automated Teller Machines (“ATMs”);
- c. Whether EMV chips would have prevented the unauthorized ATM withdrawals and other card-present transactions that class members experienced;

¹ Depo. Tr. of the Bank’s Rule 30(b)(6) Designee Robert Chestnut (“Chestnut Tr.”) 54:19-24, 75:8-13, 76:3-7, 129:2-13.

² Depo. Tr. of the Bank’s Rule 30(b)(6) Designee William Matthew Martin (“Martin Tr.”) 65:4-14.

- d. Whether the Bank's failure to equip EDD cards with EMV chips subjected class members to an increased risk of unauthorized access and exfiltration, theft, or disclosure of the cardholder's personal information; and
- e.
- f. Whether, between late September 2020 and June 2021, it would have been reasonable for the Bank to assume that all or almost all EDD debit cardholders who reported an unauthorized ATM withdrawal were likely fraudsters making false reports, rather than actual victims of counterfeit card fraud.

II. SUMMARY OF EXPERT QUALIFICATIONS

4. I have over 35 years of experience working in financial services, specifically in the payments industry, which coordinates the exchange of money for goods between customers, businesses, and financial institutions. My primary focus within the payments sector has been on product innovation for credit and debit cards, including EMV chips, contactless and mobile payments.

5. From 1982 to 1985, I worked for First Interstate Bancorp in its strategic planning group. In 1985, I joined Edgar, Dunn & Company, a consulting firm with particular expertise in the payments sector. In 2017, I joined Accenture, a large global technology and strategy consulting firm, as a Senior Managing Director in its payments industry practice. I largely retired in February 2019 but continue to work as an independent consultant.

6. In those capacities, I have gained expertise in the economic and operational aspects of the payments industry. I have assisted clients in preparing product roadmaps, strategic plans, and business cases (justifications for proposed projects based on expected commercial benefit) for new products and technology investments, including EMV chips. I have completed numerous client projects involving multiple payment methods such as credit, debit, prepaid, and

person-to-person payments. My consulting experience includes advising clients on the use of mobile payments and contactless cards and conversion to EMV chip cards.

7. Between approximately 2004 and 2015, my focus was on the business implications of EMV chip technology. I worked with Interac (Canada's debit network) to develop the business case for EMV migration for the debit in Canada. I also worked with MasterCard and Visa in the U.S. to develop industry-wide business cases for both debit and credit cards in the U.S. My work involved creating models that captured the costs (including chip and card production costs, point of sale terminal, and ATM upgrade or replacement costs, and expenses related to changes to software) and the benefits (primarily reduction of card-present counterfeit fraud) for each of the major constituents of the payments landscape: issuers, acquirers, ATM operators, merchants, networks, and processors.³ I also developed fraud

³ An issuer is a financial institution that provides payment cards, credit, debit or pre-paid, to their consumer customers. Issuer responsibilities include marketing their card products, underwriting the credit risk of each applicant, processing cardholder purchase requests, and managing the cardholder account (e.g. maintaining a record of transactions, payments, balance outstanding, etc.).

An acquirer is a financial institution that provides processing and settlement services to merchants/businesses. Acquirers enter into contracts with merchants to provide payment processing services. They maintain the merchant's account record (including individual transaction details), submit daily settlement to the network, and process the incoming receipt of funds to ensure that they are accounted appropriately. Acquirers are also responsible for underwriting each of their merchant customers.

An ATM operator is the Financial Institution or independent operator responsible for the management of the ATM, including providing services such as loading cash, ATM maintenance, ATM ownership and leasing.

Merchants provide goods and services to cardholders and submit card transactions to their acquirer for payment. Merchants are the customers of the acquirers.

Networks, also known as brands, card networks, or payment schemes, provide the infrastructure, rules, and standards necessary to process payments. They connect all the players, oversee the payment processing activity, monitor the settlement of transactions, and regulate and manage the corresponding compliance policies. The network has commercial relationships only with the issuer and the acquirer. In this case the network is Visa.

forecasts for the status quo (no EMV chips) and for the transition to the use of EMV chips for each business case. My work informed my clients' decisions regarding EMV conversion.

8. I have spoken at numerous industry conferences on topics related to payment card innovation including EMV chip technology as well as other developments related to adoption of contactless and mobile payments.

9. I have an MBA from UCLA's Anderson School of Management in Los Angeles and a BS in Economics from University of Tennessee in Knoxville.

10. A true and correct copy of my current curriculum vitae (CV), which includes a list of all publications I have authored or co-authored in the last 10 years, is attached as **Appendix A**. I have not testified as an expert at trial or by deposition in the last four years.

III. HOURLY RATE

11. I am being compensated at a rate of \$450 per hour for my work in this matter. My compensation is not contingent on the nature of my opinions or on the outcome of this litigation.

IV. FACTS AND DATA CONSIDERED

12. In preparing this report and forming the opinions expressed herein, I considered documents, testimony, and information produced in discovery in this litigation as well as publicly available documents and information and my general knowledge, training, and experience from over 30 years in the payments industry. The specific materials I considered are cited in this report and in the attached **Appendix B**.

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

Processors manage the systems that process card transactions on behalf of their customers, either issuers or acquirers. They handle the technical aspects of authorizing, clearing and settling transactions between acquirers and issuers, and manage the corresponding compliance.

V. SUMMARY OF OPINIONS

14. Based on my general knowledge, training, and over 35 years of industry experience, my review and analysis of documents produced by the Bank in this litigation and documents publicly available, and my review of the deposition testimony of the Bank's Rule 30(b)(6) designees, it is my opinion that:

- a. Payment cards that have only a magnetic stripe to hold cardholder information and not an EMV chip ("mag-stripe only cards"), including the Bank's EDD debit cards at issue in this litigation, are highly vulnerable to card skimming and card-present counterfeit fraud.
- b. The EMV standards, released in 1996, were designed to prevent card-present counterfeit fraud related to mag-stripe only cards, and EMV chips are highly effective at preventing card-present counterfeit fraud.
- c. By at least 2019, the use of EMV chips was an industry-standard security measure throughout the U.S. debit card market, including for debit cards used for the administration of government benefits.
- d. The Bank's failure to include EMV chips in its EDD debit cards was inconsistent with industry standard practices and caused those cards to be less secure and more vulnerable to skimming and card-present counterfeit card fraud (including unauthorized ATM withdrawals) than are debit cards with embedded EMV chips.
- e. The Bank's failure to include EMV chips in its EDD debit cards created an inferior level of card security for EDD debit cardholders compared to the level of card security the Bank provided to its non-prepaid consumer and business credit and debit cardholders, to whom the Bank issued EMV chip cards from 2014 onward.

- f. Given the well-known fact that criminals probe for security weaknesses and exploit vulnerabilities they identify, and that by 2020 it was well documented that fraud had begun to concentrate on mag-stripe only cards, it was highly foreseeable that card-present counterfeit fraud (including unauthorized ATM withdrawals) targeting EMV chip-less Bank-issued EDD debit cards would continue to increase during 2020. Because prepaid cards with high load values and low security are particularly attractive to criminals and because the COVID-19 pandemic was projected to result in a large increase of the EDD debit card load, it was also highly foreseeable that fraud targeting EDD cards would continue to increase during the pandemic.
- g. Skimming and card-present counterfeit fraud targeting California EDD cards increased as a result of the Bank's failure to issue EMV-chip-enabled cards and greatly increased the likelihood of unauthorized access, use, and disclosure of class member personal information.
- h. Card skimming results in the unauthorized access and exfiltration, theft, or disclosure of the cardholder's personal information.
- i. Card skimming is the best explanation for the type of fraud class members experienced on their EDD cards in 2020-2021.
- j. The addition of EMV chips to the Bank's EDD debit cards would have prevented virtually all the card-present counterfeit fraud (including unauthorized ATM withdrawals) that class members experienced.
- k. Any major financial institution in the Bank's situation in 2020-21 would have known that many EDD debit cardholders who reported unauthorized ATM

withdrawals during the pandemic were true victims of card skimming and/or card-present counterfeit card fraud.

VI. STATEMENT OF OPINIONS AND BASIS FOR OPINIONS

A. Mag-Stripe Only Cards Are Highly Vulnerable to Skimming and Card-Present Counterfeit Fraud.

15. Prior to July 2021, all Bank-issued EDD debit cards were mag-stripe only debit cards.⁴

16. IBM created the first mag-stripe card in the 1960s.⁵ IBM essentially attached magnetic recording tape, invented in Germany in the 1920s, to a card, which was originally used for entry control.⁶ In 1970, American Express was the first to use mag-stripe cards for payments, using the magnetic recording tape to store personal information regarding the cardholder, including the cardholder's name, and credit card number, and data relevant to the payment, such as the card expiration date.

17. Mag-stripe payment cards typically have three tracks on the mag-stripe. Tracks 1 and 2 are used to store data specified by the card brand (e.g., Visa) in pre-specified formats, while Track 3 is used primarily for additional information specified by the issuer.⁷ The data on the three tracks does not change from one transaction to the next and is easily readable.⁸ The

⁴ Martin Tr. 65:8-14.

⁵ See The Magnetic Stripe, IBM, <https://www.ibm.com/history/magnetic-stripe#:~:text=Parry%20helped%20develop%20the%20Universal,It%20worked> (last accessed Aug. 7, 2024).

⁶ See Vicki Hyman, Swiping Left on Magnetic Stripes, VISA Newsroom (Aug. 12, 2021), <https://www.mastercard.com/news/perspectives/2021/magnetic-stripe/>.

⁷ See Jerome Svigals, The Long Life and Imminent Death of the Mag-Stripe Card, IEEE Spectrum (May 30, 2012), <https://spectrum.ieee.org/the-long-life-and-imminent-death-of-the-magstripe-card>.

⁸ See *id.*

Motley Fool, a private investment advisory firm for individuals, has described the process as follows:⁹

Cards [...] store all pertinent data on the magnetic stripe on the back of the card, including the cardholder's name, credit card number, expiration date, and CVV number. Once the information is written on this stripe, however, it is forever static, meaning it will never change.

18. Card-present counterfeit fraud occurs when criminals use a cloned card to make purchases or ATM withdrawals that are charged to the real cardholder's account. Criminals obtain the card data through various scams, including a process called "skimming." Skimming occurs when criminals surreptitiously install a device capable of reading the information on a magnetic stripe on an ATM's card reader and a pinhole camera or PIN pad overlay to capture the cardholder's Personal Identification Number ("PIN") alongside their card data. The individuals later retrieve and use the stolen data to manufacture and use counterfeit or "cloned" cards.

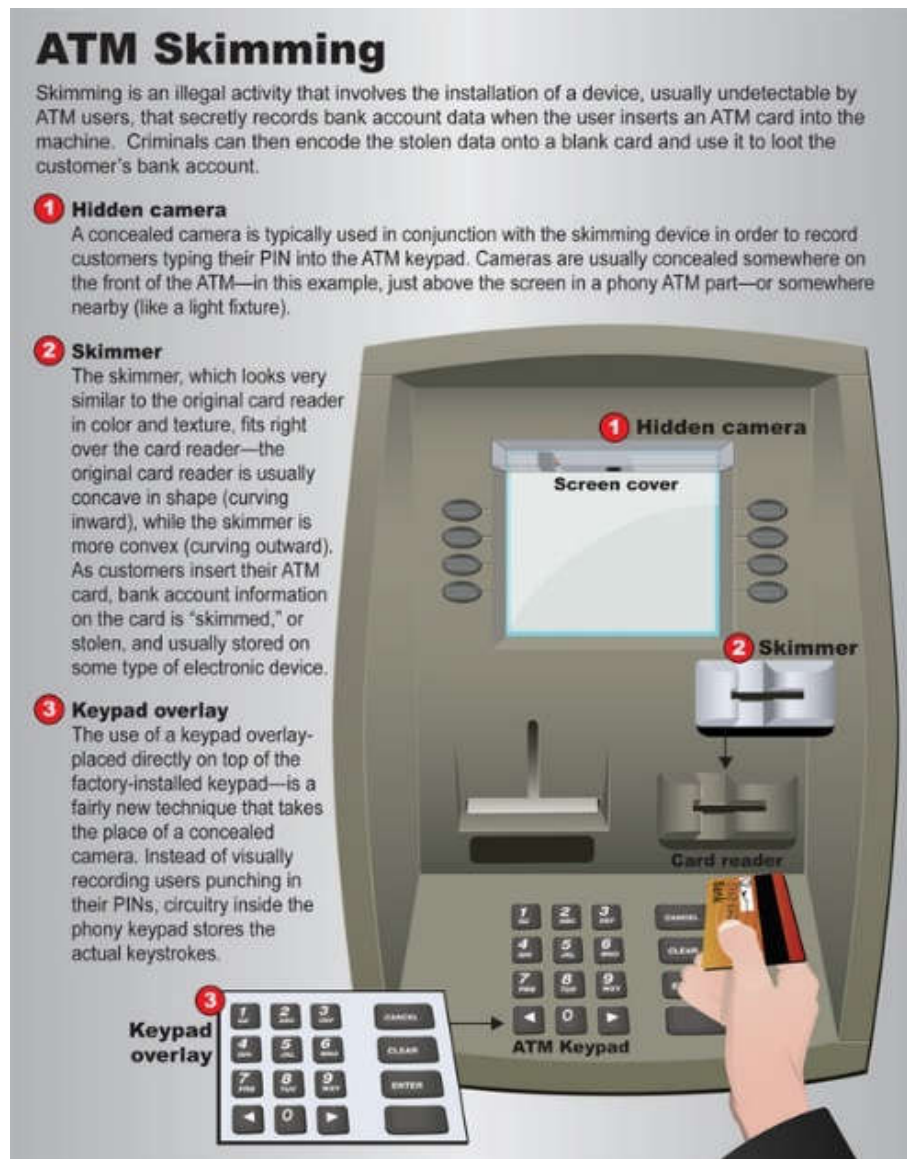
19. As part of most skimming operations, pinhole cameras or PIN pad overlays capture the PIN as the unsuspecting cardholder enters it into the payment terminal or ATM. Using data from the mag stripe and the PIN together, the criminal can manufacture counterfeit cards to then make unauthorized purchases or ATM withdrawals.

20. The following graphic from the FBI identifies several common skimming devices and where they would typically be placed on an ATM.¹⁰

⁹ Matthew Cochrane, Why U.S. Counterfeit Credit Card Fraud Is Down 75%, Motley Fool (Sept. 17, 2018, 5:11 PM), <https://www.fool.com/investing/2018/09/16/why-us-counterfeit-credit-card-fraud-is-down-75.aspx>.

¹⁰ Taking a Trip to the ATM, Beware of 'Skimmers', FBI News (July 14, 2011), <https://www.fbi.gov/news/stories/atm-skimming>.

FBI Overview of ATM Skimming



21. Pinhole cameras (Item 1 on the FBI's Overview of ATM Skimming) are very small and are often disguised in side panels or trim pieces attached to the ATM. Below is an example of what a pinhole camera looks like:¹¹

¹¹ Photos: How to Detect Skimming Devices on ATM's [sic], CBS21 News (March 15, 2018, 10:50 AM), <https://local21news.com/news/local/photos-how-to-detect-skimming-devices-on-atms>.

Pinhole Camera Example:



22. Item 2 on the FBI's Overview of ATM Skimming describes a skimmer, the device that reads the mag stripe and captures the card details for the criminal to gather later after collecting details from many cards.¹² Below is an example of a card skimmer, installed and partially opened: ¹³

ATM Card Skimmer, Installed and Partially Opened



¹² See Taking a Trip to the ATM, Beware of 'Skimmers', FBI News (July 14, 2011), <https://www.fbi.gov/news/stories/atm-skimming>.

¹³ See Brian Krebs, Why I Always Tug on the ATM, Krebs on Security (March 31, 2017), <https://krebsonsecurity.com/2017/03/why-i-always-tug-on-the-atm/>.



Appearance of skimmer from outside ATM.	The skimmer overlay when removed.
---	-----------------------------------

23. A PIN pad overlay (Item 3 on the FBI's Overview of ATM Skimming above)¹⁴ is an alternative to using a pinhole camera. It is inserted over the real PIN pad and captures the PIN number using the sensors on the back side of the device. Below is an example of a PIN pad overlay.¹⁵

Example of Pin Pad Overlay

24. The skimmers, PIN pad overlays, and pinhole cameras are very realistic, making them very hard to spot. The picture below depicts an ATM that is compromised compared to one that has not been compromised, showing how hard it may be to spot the skimming and PIN capture devices:¹⁶

¹⁴ Taking a Trip to the ATM?: Beware of 'Skimmers', FBI News (July 14, 2011), <https://www.fbi.gov/news/stories/atm-skimming>.

¹⁵ Understanding Card Skimmers and How to Protect Yourself, Los Angeles County Consumer & Business Affairs (April 17, 2023), <https://dcba.lacounty.gov/newsroom/understanding-card-skimmers-and-how-to-protect-yourself/> (attributing the photo to Sean Cooper, What You Need to Know About Card Skimming, Engadget (July 28, 2014), <https://www.engadget.com/2014-07-28-credit-card-skimming-explainer.html>).

¹⁶ ATM Skimming Gets a Tech Upgrade, PYMTS (Sept. 18, 2017), <https://www.pymnts.com/news/security-and-risk/2017/atm-skimming-gets-a-tech-upgrade/>.

Card Skimmer on ATM



25. Once the criminal has implanted the skimmer and PIN pad overlay or camera, the skimmer records the information from the mag-stripe while the PIN pad overlay or camera captures the PIN.¹⁷ The criminal can then use this information to create a counterfeit card, which functions the same as the original mag-stripe only card and can be used in conjunction with the stolen PIN to make fraudulent card-present transactions, including unauthorized ATM withdrawals.¹⁸

26. Counterfeit fraud due to skimming has long been a well-known problem throughout the payment services industry and law enforcement. Skimmers have been used since as early as December 2002,¹⁹ but “ATM skimming really began to take off globally in 2010 with the large-scale production of skimming devices, especially the wireless variety.”²⁰ When “3-D printing came along in 2011, high-quality skimming devices became even simpler to produce,

¹⁷ See Taking a Trip to the ATM?: Beware of ‘Skimmers’, FBI News (July 14, 2011), <https://www.fbi.gov/news/stories/atm-skimming>.

¹⁸ See What Is Credit Card Fraud?, Equifax, <https://www.equifax.com/personal/education/credit-cards/articles/-/learn/credit-card-fraud/>.

¹⁹ Sue Chan, Is Your Credit Card Being Skimmed?, CBS News (Dec. 6, 2002, 3:46 PM), <https://www.cbsnews.com/news/is-your-credit-card-being-skimmed/>.

²⁰ Yossi Geller, ATM Fraud: The Evolution of An Epidemic, ATM Marketplace (Dec. 13, 2016), <https://www.atmmarketplace.com/articles/atm-fraud-the-evolution-of-an-epidemic/>.

with razor-thin Bluetooth-compatible versions replacing clunky overlays.”²¹ ATM Marketplace, an ATM industry news and information website, reported in 2016: “ATM skimming is a growing epidemic that shows no sign of slowing.”²² Fair Isaac Corporation (“FICO”) reported a six-fold increase in compromises of ATMs and merchant devices in the United States in 2015 and predicted continuing increases: “As the last few years have proven, skimming technology and knowhow have improved and are more accessible to the general population, so we will continue to see increases in compromises and the speed at which they occur.”²³

27. Counterfeit fraud is a significant problem. In 2015, the Nilson Report, a payments industry newsletter, estimated total U.S. counterfeit fraud to be \$3.89 billion.²⁴ This number includes data stolen from multiple points of compromise including skimming as well as data breaches.²⁵ The FBI has estimated that skimming alone “costs financial institutions and consumers more than \$1 billion each year.”²⁶

28. Through skimming, criminals gain access to all information stored on the magnetic stripe, including the cardholder’s unencrypted personal information, such as name and card number. Skimming thus presents one well-documented means of unauthorized access and theft of unencrypted personal information. Counterfeit fraud resulting from skimming is,

²¹ *Id.*

²² *Id.*

²³ FICO Reports a 70 Percent Rise in Debit Cards Compromised at U.S. ATMs and Merchants in 2016, Fraud Protection & Compliance, FICO (Mar. 29, 2017), <https://www.fico.com/en/newsroom/fico-reports-70-percent-rise-debit-cards-compromised-u-s-atms-and-merchants-2016>.

²⁴ Global Card Fraud Losses Reach \$16.31 Billion – Will Exceed \$35 Billion in 2020 According to The Nilson Report, Business Wire (Aug. 4, 2015, 7:49 PM), <https://www.businesswire.com/news/home/20150804007054/en/Global-Card-Fraud-Losses-Reach-16.31-Billion#.VgDIZRFViko>; Card Fraud Losses Reach \$16.31 Billion, Nilson Report (August 2015), <https://nilsonreport.com/articles/card-fraud-losses-reach-16-31-billion/>.

²⁵ Card Fraud Losses Reach \$16.31 Billion, Nilson Report (August 2015), <https://nilsonreport.com/articles/card-fraud-losses-reach-16-31-billion/>.

²⁶ How We Can Help You, Skimming, FBI, <https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/skimming> (last visited Aug. 1, 2024).

similarly, a well-documented means of using personal data, and requires disclosure of such data to carry out any transaction (to communicate with the issuer to verify the transaction), including an ATM withdrawal.

B. EMV Chips Are Extremely Effective at Preventing Card-Present Counterfeit Fraud.

29. EMV chip cards prevent card-present counterfeit fraud by employing an embedded EMV chip that creates a *dynamic*, as opposed to static code, often called a dynamic CVV code, that is unique to each transaction.²⁷ As described below, EMV chips themselves, which are required to generate a dynamic CVV code, are next to impossible to counterfeit. As a result, the personal data transmitted in EMV chip transactions, unlike that on static mag-stripe-only cards, cannot be used to make counterfeit cards capable of carrying out normal transactions.

30. An EMV chip uses information provided by the point of sale (“POS”) terminal (for example the terminal ID/location or amount of purchase) as well as data from the card (for example, the cardholder name, account number, or expiration date) to create an encrypted code (the dynamic CVV code) that is unique to each transaction. The dynamic CVV code is then included in the authorization request created by the card.²⁸

31. When the issuer receives the electronic request for authorization from the terminal, the issuer can immediately confirm based on its own records and the codes provided whether the card has an embedded EMV chip, and whether the data in the authorization request

²⁷ The term “EMV” is derived from the names of the original collaborators who developed the EMV standards governing all EMV chips—EuroPay, MasterCard and Visa (EuroPay later merged with MasterCard). EMVCo is the organization responsible for managing the EMV standards as well as other global payment security standards. EMVCo is governed by the payment networks and payment industry participants. *See generally* The Role of the EMV® Specifications, EMVCo (Mar. 18, 2020), <https://www.emvco.com/knowledge-hub/the-role-of-the-emv-specifications-2/>.

²⁸ *See generally* EMV At a Glance, EMVCo (2022), <https://www.emvco.com/wp-content/uploads/2022/09/EMV%C2%AE-Chip-At-A-Glance-EMVCo-eBook.pdf>; A Guide to EMV Chip Technology, EMVCo (Nov. 2014), <https://www.fisglobal.com/-/media/fisglobal/WorldPay/Docs/Insights/A-Guide-to-EMV-Chip-Technology.pdf>.

came from that chip or from the mag-stripe. If the correct dynamic CVV code is not presented, the transaction can either be declined or subject to additional and extremely strict security rules specific to “fallback transactions,” which I explain in more detail below. Again, as described below, an issuer is incentivized to decline such transactions to avoid losses associated with any potential fraud related to fallback transactions.²⁹

32. The correct dynamic CVV code cannot be successfully created without a legitimate EMV chip. And EMV chips are next to impossible to clone because they contain private keys that are never transmitted and thus cannot be compromised (extracted or copied).³⁰ EMV technology thus largely protects against the creation of functional counterfeit cards, and thereby protects against the use of data captured in a skimming attack to facilitate counterfeit fraud.

33. EMV chip cards still include the traditional mag stripe, and criminals can skim the mag stripe data (discussed above) to create a mag stripe-only version of the EMV card. Notably, EMV technology was not designed to prevent the capture of mag-stripe data – it was designed to disrupt the *use* of that data via card cloning or counterfeit.

34. As a result, it is possible to create a counterfeit mag-stripe only version of an EMV chip card, but that card cannot be *used* to make a normal transaction in any terminal that has a chip reader (which includes virtually all ATMs and the vast majority of point of sale terminals). The mag stripe on an EMV chip card contains a service code that indicates that the card has an EMV chip. If a counterfeit mag-stripe only version of an EMV chip card is swiped so that the EMV capable terminal reads the mag stripe, the mag stripe on the card transmits that code to the terminal to indicate that a chip has been embedded on the card. If the transaction

²⁹ See *infra* ¶ 37 (describing liability shift rules).

³⁰ U.S. Payments Forum, Debunking EMV Myths, at 6 (2019), <https://www.uspaymentsforum.org/wp-content/uploads/2019/03/Debunking-EMV-Myths-March-2019.pdf> (“EMV chip cards, [sic] have multiple measures to prevent external access and copying of its keys. Without the chip’s cryptographic keys, it’s not possible to create a functioning counterfeit version of a chip card to be used through the contact or contactless interfaces.”).

proceeds using the mag stripe, no correct CVV code will be transmitted, and the only transaction that is possible is a “fallback” transaction.³¹

35. A “fallback transaction” occurs when, instead of declining a transaction, the ATM or POS terminal allows the cardholder to “fallback” and use the mag-stripe of a detected chip card to make the transaction. When allowing a fallback transaction, the ATM or POS terminal will typically send a code within the authorization request to the card issuer notifying the issuer that a mag-stripe transaction has been requested with a chip card. If they do not include the fallback code, the liability for any fraudulent fallback transactions falls on the merchant or ATM operator.³²

36. Fallback transactions are generally limited by significant security measures over which card issuers exercise control. The issuer can require additional security checks, decline a fallback transaction, or approve a transaction with or without withdrawal limits. If the merchant or ATM operator provides this fallback notice code to the issuer and the issuer authorizes the fallback transaction, then liability for the fallback transaction, if it proves to be fraudulent, falls on the issuer.

37. The number of fallback transactions was a concern during the initial years of EMV deployment, largely due to problems with implementation. As a result, 75% of card issuers rolled out new policies to “decline authorization of high-dollar fallback purchases,” while others focused on merchants with abnormally high fallback rates and other methods to control

³¹ Mag stripes on chip enabled cards contain a service code that indicates that a chip is on the card. If that chip card is swiped so that the mag stripe is used instead of the chip, the chip enabled terminal may reject the transaction and request that the cardholder resubmit using the chip instead of the mag stripe. In some instances, for example when the chip is unreadable, issuers may allow a transaction to proceed with mag-stripe only data.

³² EMV Implementation Guidance: Fallback Transactions, US Payments Forum 1 (2016), <https://www.uspaymentsforum.org/wp-content/uploads/2017/03/Fallback-Transaction-Guidance-FINAL-Dec-2016.pdf>; Ann Davidson, *Fraud & Fallback: What You Need to Know About Skimming Attacks*, Credit Union Times (Sept. 16, 2024), <https://www.cutimes.com/2024/09/16/fraud-fallback-what-you-need-to-know-about-skimming-attacks/?slreturn=20241116-43702>.

the use of fallbacks.³³ However, by 2017, fallback transactions represented less than 2% of overall purchase authorizations and fraud related to those transactions was falling rapidly as a result of industry mitigation efforts, including the use of fallback rules.³⁴ In addition to issuer-specific fallback rules, both Visa and MasterCard impose transaction fees to penalize frequent fallback transactions. If fallback transactions at a given ATM exceed 2.5% for Visa or 3.0% for Mastercard, the networks impose penalty fees.³⁵ The penalty fees imposed by the networks provide merchants and ATM operators with an economic incentive to ensure that their equipment is properly functioning and to investigate any increases in fallback rates.

38. In 2018, fraud data showed that fallback fraud represented only 11.5% of counterfeit fraud, down from more than 20% in 2017, and only 3.2% of overall credit card fraud, down from 4.5% in 2017, declines of 45% and 30% year over year.³⁶

39. Fraudulent transactions carried out through “fallback” mechanisms are, in sum, infrequent as a result of strict limitations by issuers and the industry. As a result, fallback transaction fraud has not limited the extreme efficacy of EMV chips at preventing card-present counterfeit fraud in any significant way.

40. For these reasons, “skimming” attacks that attempt to steal personal information from the EMV chip itself are also unable to generate a successful clone of an EMV card that can

³³ Credit Card “Fallback” Fraud Declines Significantly as Banks Implement New Policies, Auriemma Roundtables: Industry Analysis (Nov. 7, 2018), <https://roundtables.us/credit-card-fallback-fraud-declines-significantly-as-banks-implement-new-policies/>.

³⁴ *Id.*; Ann Davidson, Fraud & Fallback: What You Need to Know About Skimming Attacks, Credit Union Times (Sept. 16, 2024), <https://www.cutimes.com/2024/09/16/fraud-fallback-what-you-need-to-know-about-skimming-attacks/?slreturn=20241116-43702> (“Both chip cards and readers undergo rigorous testing and certification, making fallback incidents exceptionally rare.”).

³⁵ *Id.*

³⁶ Credit Card “Fallback” Fraud Declines Significantly as Banks Implement New Policies, Auriemma Roundtables: Industry Analysis (Nov. 7, 2018), <https://roundtables.us/credit-card-fallback-fraud-declines-significantly-as-banks-implement-new-policies/>.

be used to carry out fraudulent ATM withdrawals or other transactions. Shimmers are paper-thin devices that are inserted into the chip card reader. Fraud rings place a shimmer inside the chip card reader to record the information transmitted between the chip and the ATM or POS terminal. Shimming devices capture the *one-time* dynamic code (making it fixed and static, not dynamic and ever-changing) and other cardholder data that an EMV chip card transmits to an ATM or POS terminal during that particular transaction. Fraudsters then copy the chip data, including the previously used one-time chip code, onto the magnetic stripe of a counterfeit card. Shimmers do not enable the dynamic-functioning EMV chip itself to be cloned and thus cannot generate the correct dynamic CVV code for subsequent transactions.

41. In 2016, NCR Corporation, one of the largest ATM manufacturers, described shimming in an alert to customers and wrote: “The only way for this attack to be successful is if a [bank card] issuer *neglects to check the CVV* when authorizing a transaction.”³⁷ The alert continued: “All issuers **MUST** make these basic checks to prevent this category of fraud. Card Shimming *is not a vulnerability with a chip card, nor with an ATM*, and therefore it is not necessary to add protection mechanisms against this form of attack to the ATM.”³⁸

42. Generally, because EMV chips cannot be successfully counterfeited and are required to create the correct dynamic CVV, card-present counterfeit fraud can be effectively prevented by including EMV chips on credit, debit and ATM cards. As Javelin Consulting reports: “*Chip cards have proven to lower fraud at the point of sale as they effectively eliminate*

³⁷ KrebsOnSecurity, ATM ‘Shimmers’ Target Chip-Based Cards (Jan. 27, 2017), <https://krebsonsecurity.com/2017/01/atm-shimmers-target-chip-based-cards/> (emphasis added).

³⁸ *Id.* (emphasis added); *see also* U.S. Payments Forum, Debunking EMV Myths, at 6 (2019), <https://www.uspaymentsforum.org/wp-content/uploads/2019/03/Debunking-EMV-Myths-March-2019.pdf> (noting that without an EMV “chip’s cryptographic keys, it’s not possible to create a functioning counterfeit version of a chip card to be used through the contact or contactless interfaces” as “[i]ssuers applying appropriate security controls easily determine counterfeit attempts and block such transactions, rendering [mag-stripe only counterfeit] cards useless.”).

counterfeiting. They cryptographically prevent criminals from forging the plastic and using those fake cards at merchant locations.”³⁹

43. In April 2018, a study by the ATM Industry Association found that “[t]he vast majority (91 percent) of U.S. ATMs are now EMV-capable, and fully 86 percent accept chip-on-chip transactions.”⁴⁰ Thus, by early 2018, most ATMs in the United States required the use of an EMV chip at an ATM when an EMV chip is present on the card, and even more were to be certified and tested to do so shortly.

44. As EMV technology became widespread, use of EMV chips has successfully and significantly reduced fraud around the world, as the examples in the chart below show:

Country	Time	Counterfeit Fraud Change	Comments
UK Debit & Credit Full Implementation ($>90\%$) ⁴¹	2008 - 2019	↓90% ⁴²	“Counterfeit card losses totaled £16.3 million in 2018, a decrease of 33 per cent compared to 2017 and 90 per cent lower than the peak reported in 2008 (£169.8 million).” ⁴³

³⁹ From Application to Transaction: Card Fraud Trends, Threats, and Tactics, JAVELIN at 6 (April 2018), <https://javelinstrategy.com/sites/default/files/files/reports/18-5006J-FM-From%20Application%20to%20Transaction-FIS.pdf> (emphasis added).

⁴⁰ Nearly All US ATMs Now EMV-Capable, Study Finds, ATM Marketplace (April 6, 2018), <https://www.atmmarketplace.com/news/nearly-all-us-atms-now-emv-capable-study-finds/>. The five percent gap between EMV-capable and ATMs prepare to accept chip-on-chip transactions “represents the lag in certification and testing” required to ready an EMV-capable ATM for chip-on-chip transactions.” ATM Industry Association, 2018 ATMIA EMV Migration Survey: Executive Summary (2018), *available at* <https://www.atmmarketplace.com/>.

⁴¹ Alex Rolfe, US Market Hits 1 Billion EMV Chip Cards Milestone, Payments Cards & Mobile (June 1, 2020), <https://www.paymentscardsandmobile.com/us-market-hits-1-billion-emv-chip-cards-milestone/>.

⁴² Fraud the Facts 2019, UK Finance at 17 (2019), <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202019%20-%20FINAL%20ONLINE.pdf>.

⁴³ *Id.*

Country	Time	Counterfeit Fraud Change	Comments
Canada Debit Full Implementation (>90%) ⁴⁴	2008 - 2015	↓92% ⁴⁵	Canada began its chip-and-PIN conversion in 2008 and completed the debit card conversion in 2012. Debit fraud losses from skimming peaked at CA\$142.3 million in 2009, but by 2015 are down by 92%. ⁴⁶
US Partial Implementation Debit & Credit (~80%)	2015 - 2019	↓87% at EMV merchants ↓62% at all US merchants ⁴⁷	Additionally, the Federal Reserve Bank of Atlanta reported in June 2019 that “counterfeit card fraud is dropping [...] [in] a trend in that direction that is consistent with the [other] countries” that had previously migrated to EMV chip. ⁴⁸

45. Even with only 80% of merchant terminals converted in 2019, the U.S. was already seeing 87% decreases in fraud at merchants that had converted and 62% at all merchants, including those who had not yet converted, as compared to fraud levels four years earlier.⁴⁹ As Helcim, a payment services provider focused on small businesses, reported to its customers:⁵⁰

⁴⁴ Alex Rolfe, US Market Hits 1 Billion EMV Chip Cards Milestone, Payments Cards & Mobile (June 1, 2020), <https://www.paymentscardsandmobile.com/us-market-hits-1-billion-emv-chip-cards-milestone/>.

⁴⁵ Jim Daly, With Its EMV Conversion Nearly Complete, Canada’s POS Debit Fraud Falls to New Low (Feb. 25, 2016), <https://www.digitaltransactions.net/with-its-emv-conversion-nearly-complete-canadas-pos-debit-fraud-falls-to-new-low/>.

⁴⁶ *Id.*

⁴⁷ Visa EMV Chip Cards Help Reduce Counterfeit Fraud by 87 Percent, Visa (Sept. 3, 2019, 3:48 PM), <https://usa.visa.com/visa-everywhere/blog/bdp/2019/09/03/visa-emv-chip-1567530138363.html>.

⁴⁸ Douglas King, The Future of U.S. Fraud in a Post-EMV Environment, Retail Payments Risk Forum at 22 (June 2019), <https://www.atlantafed.org/-/media/documents/rprf/publications/2019/06/23/future-of-us-fraud-in-post-emv-environment-king-doug.pdf>.

⁴⁹ Visa EMV Chip Cards Help Reduce Counterfeit Fraud by 87 Percent, Visa (Sept. 3, 2019, 3:48 PM), <https://usa.visa.com/visa-everywhere/blog/bdp/2019/09/03/visa-emv-chip-1567530138363.html>.

⁵⁰ Danny Randell, EMV Chip Cards: Everything You Need to Know, Helcim Blog (Aug. 17, 2022), <https://www.helcim.com/guides/emv-chip-card-technology/>.

When EMV cards were first introduced, they had a significant impact on payments fraud because of these unique, dynamic data transaction IDs which cannot be replicated. As an example, in the US, it is estimated that from 2015 to 2018, card-present credit card fraud fell by as much as 75% due to the enhanced security of EMV chip technology.⁵¹

C. By At Least 2019, EMV Chips Were the Industry Standard for Credit and Debit Card Security.

46. EMV chip technology standards have existed since 1996. By 2013, EMVCo's membership had expanded beyond the original members (Europay, Mastercard and Visa) to include participation by all major stakeholder groups, including the principal global card brands: JCB joined in 2004, American Express joined in 2009, followed by Discover and UnionPay in 2013.⁵² Participation also expanded to include a broad range of interested industry stakeholders, including merchants, payment processors and other payments industry companies.

47. The first major payments market to convert to EMV chips was the UK, which in May 2003 began EMV trials and on February 14, 2006 converted nationwide. Shortly thereafter, other countries began implementing EMV. By 2019, over 8.8 billion EMV chip cards had been issued in Europe, Africa and the Middle East, Canada, and Latin America and the Caribbean, and each of those regions had over 90% of their transactions processed with EMV chips.⁵³

48. In October 2010, United Nations Federal Credit Union became the first U.S. issuer to offer EMV cards to its credit customers.⁵⁴ Other U.S. banks soon followed, issuing EMV credit cards to selected segments of their customers, including those with frequent international travel.

⁵¹ A 75% reduction is consistent with Visa data from three months prior, March 2019, as compared to the data referenced in the chart above.

⁵² Why EMV?, EMVCO, <https://www.emvco.com/why-emv/> (last visited Feb. 27, 2025).

⁵³ Alex Rolfe, US Market Hits 1 Billion EMV Chip Cards Milestone, Payments Cards & Mobile (June 1, 2020), <https://www.paymentscardsandmobile.com/us-market-hits-1-billion-emv-chip-cards-milestone/>.

⁵⁴ Saurabh Kumar Choudhary, EMV Compliance in the U.S., Capgemini at 17 (2012), https://www.capgemini.com/wp-content/uploads/2017/07/EMV_Compliance_in_the_U.S..pdf (citing EMV Resources, Secure Technology Alliance, <https://www.securetechalliance.org/smart-cards-applications-emv/>).

49. By mid 2012, the U.S. payments market committed to migrating to EMV. MasterCard, Visa, American Express, and Discover each issued “liability-shift” rules that took effect in October 2015.⁵⁵ Liability-shift rules were used in many countries to create economic incentives for issuers and merchants to adopt EMV technology. A liability-shift rule assigns liability for fraud to whichever party (either the card issuer or the acquirer/merchant) has the least protection.⁵⁶ For example, if a mag-stripe only card is presented to an EMV capable merchant, the issuer of that card bears the cost of any fraud associated with that transaction. The opposite would be true if an EMV card is presented to a mag-stripe only reader—the merchant rather than the issuer would be liable for any fraud. If the mag-stripe on an EMV capable card is used on an EMV capable reader and the merchant has configured its terminal to accept the mag-stripe rather than forcing use of the chip (as is industry standard practice), the merchant is liable for any resulting fraud because the merchant allowed the less secure technology to be used.

⁵⁵ EMV in the USA: The Story So Far, American Banker (April 5, 2013, 3:27 PM), <https://www.americanbanker.com/payments/slideshow/emv-in-the-usa-the-story-so-far>.

For additional information see: Understanding the U.S. EMV Liability Shifts, US Payments Forum at 4-5 (July 2017), <https://www.uspaymentsforum.org/wp-content/uploads/2017/07/EMV-Fraud-Liability-Shift-WP-FINAL-July-2017.pdf>.

⁵⁶ *See id.*

50. Shortly after the announcement of liability-shift rules and deadlines, several major U.S. banks, including Bank of America, announced plans to issue cards with embedded EMV chips for their credit card portfolios.⁵⁷ The table below from Capgemini's report entitled EMV Compliance in the U.S. provides a timeline for key commitments to EMV in the U.S. announced in 2010 and 2011.⁵⁸

⁵⁷ Saurabh Kumar Choudhary, EMV Compliance in the U.S., Capgemini at 17 (2012), https://www.capgemini.com/wp-content/uploads/2017/07/EMV_Compliance_in_the_U.S..pdf (citing EMV Resources, Secure Technology Alliance, <http://www.smartcardalliance.org/pages/smart-cards-applications-emv>); Jonathan Camhi, Bank of America Switches to EMV Chip Credit Cards for Consumers, InformationWeek (July 23, 2012, 3:50 PM), <https://www.banktech.com/payments/bank-of-america-switches-to-emv-chip-credit-cards-for-consumers/d/d-id/1295590d41d.html?>

⁵⁸ *Id.*

Figure 1: EMV Compliance in the U.S.

October 2010	United Nations Federal Credit Union became the first the U.S. institution to offer its customers EMV cards
December 2010	Travelex introduced a pre-paid foreign currency Chip and PIN card denominated in Euros and pound sterling for U.S. travelers abroad
October 2010	State Employees Credit Union announced its plan to convert its entire 1-million-card debit portfolio to EMV chips
February 2011	Wells Fargo & Co., the U.S. bank with the most branches, began testing microchip-embedded credit cards with frequent travelers to address complaints of customers who have trouble using their cards abroad
July 2011	Silicon Valley Bank (SVB) began providing chip-enabled, or Smart, credit cards available to businesses in the U.S.
June 2011	The U.S. bank announced that it will offer its international travelers EMV cards
June 2011	JPMorgan Chase & Co. announced that it will begin issuing its J.P. Morgan Select Visa Signature card with EMV chip technology, the second in its card portfolio—following the J.P. Morgan Palladium Card—to sport the smart chip
June 2011	The Payment Processing Solutions (PPS) division of Jack Henry & Associates announced it will begin offering chip-and-signature debit and credit cards to its credit union customers
August 2011	PSCU Financial Services began offering its entire member-owner base of 680 credit unions new credit cards that carry both EMV chip-and-PIN security and traditional magnetic stripes
August 2011	Citi announced the launch of the Citi Corporate Chip and PIN card, a compliant smart card designed for the U.S. corporate cardholders traveling abroad
November 2011	Bank of America decided to roll out chip-and-pin business cards in 2012

51. By 2014-2015, the U.S. debit card industry had begun migration efforts to EMV.

According to the 2014 Debit Issuer study by Celent, a large global research and advisory firm focused on technology for financial institutions:

86% of the US debit issuers were planning to start issuing EMV cards in 2014-2015, with most efforts focused on 2015. The EMV Migration Forum [a cross industry body focused on the U.S. EMV transition] forecasts that 4.5 million terminals will have been installed by the end of 2014, and over 46% of US merchant terminals will be enabled for EMV by the end of 2015. In October 2014, President Obama signed an executive order to use EMV for all government cards. It is estimated that 100 million EMV chip cards will have been issued by the end of 2014. In September, Bank of America announced that all new debit cards will be

EMV. **“The US EMV train has finally left the station and is building up steam,”** said Zilvinas Bareisis, senior analyst at Celent.⁵⁹

52. On September 20, 2014, Bank of America announced it was committed to converting its consumer and commercial debit card portfolio to EMV to provide enhanced security for its customers, becoming the first major U.S. bank to add EMV chip technology to debit cards.⁶⁰ Titi Cole, retail products and underwriting executive for Bank of America, stated that “[c]hip technology is an important tool in increasing card security, and we want our customers to have the best possible experience when using their payment cards” and “[t]he new chip-enabled debit cards will improve security of customers’ transactions when traveling abroad and at home as more U.S. merchants adopt chip technology.”⁶¹ The release noted that existing Bank customers would receive chip cards when their existing cards were replaced at expiration or for any other reason and that the Bank expected to complete conversion of its consumer and small business debit cards to EMV by the end of 2015.⁶²

53. On October 17, 2014, President Obama signed an Executive Order, Improving the Security of Consumer Financial Transactions, calling for all government agencies to shift to the use of chip-and-PIN technology (i.e. EMV) credit, debit, and other payment cards, *including for all prepaid debit cards used to distribute federal government benefits*.⁶³ The switch was needed, the Order explained, to “further strengthen the security of consumer data” and “improve the security of consumer financial transactions in both the private and public sectors.”⁶⁴ The Order mandated that all executive departments and agencies must “transition payment processing

⁵⁹ US Shifts to EMV as Obama and Apple Weigh In, FinTech Futures (Dec. 15, 2014), <https://www.fintechfutures.com/2014/12/us-shifts-to-emv-as-obama-and-apple-weigh-in/> (emphasis added).

⁶⁰ Bank of America Begins Rollout of Chip Debit Cards, Business Wire (Sept. 30, 2014, 11:10 AM), <https://www.businesswire.com/news/home/20140930005292/en/Bank-of-America-Begins-Rollout-of-Chip-Debit-Cards>.

⁶¹ *Id.*

⁶² *Id.*

⁶³ Exec. Order No. 13681, 79 F.R. 63491 (Oct. 23, 2014).

⁶⁴ *Id.*

terminals and credit, debit, and other payment cards to employ enhanced security features, including chip-and-PIN technology.”⁶⁵ The mandate to transition to EMV chip cards applied to Direct Express federal programs, which provide prepaid debit cards for monthly deposits of Social Security, Supplemental Security Income, veterans, and other federal benefits and that are administered by the Treasury Department,⁶⁶ as well as credit, debit, and other payment cards provided through the General Services Administration (GSA).⁶⁷ The Executive Order directed both the Treasury Department and GSA to transition covered cards to EMV by no later than January 1, 2015. The relevant text of the Executive Order states:

Given that identity crimes, including credit, debit, and other payment card fraud, continue to be a risk to U.S. economic activity, and given the economic consequences of data breaches, the United States must take further action to enhance the security of data in the financial marketplace. While the U.S. Government's credit, debit, and other payment card programs already include protections against fraud, the Government must further strengthen the security of consumer data and encourage the adoption of enhanced safeguards nationwide in a manner that protects privacy and confidentiality while maintaining an efficient and innovative financial system.

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to improve the security of consumer financial transactions in both the private and public sectors, it is hereby ordered as follows:

Section 1. Secure Government Payments. In order to strengthen data security and thereby better protect citizens doing business with the Government, executive departments and agencies (agencies) shall, as soon as possible, transition payment processing terminals and credit, debit, and other payment cards to employ enhanced security features, including chip-and-PIN technology. In determining enhanced security features to employ, agencies shall consider relevant voluntary consensus standards and specifications, as appropriate, consistent with the National Technology Transfer and Advancement Act of 1995 and Office of Management and Budget Circular A-119.

⁶⁵ *Id.* §1.

⁶⁶ See Direct Express, Frequently Asked Questions, <https://www.usdirectexpress.com/faq.html> (last accessed Aug. 8, 2024).

⁶⁷ Exec. Order No. 13681, 79 F.R. 63491, §1 (Oct. 23, 2014).

(a) The Secretary of the Treasury shall take necessary steps to ensure that payment processing terminals acquired by agencies through the Department of the Treasury or through alternative means authorized by the Department of the Treasury have enhanced security features. No later than January 1, 2015, all new payment processing terminals acquired in these ways shall include hardware necessary to support such enhanced security features. By January 1, 2015, the Department of the Treasury shall develop a plan for agencies to install enabling software that supports enhanced security features.

(b) The Administrator of General Services shall take necessary steps to ensure that **credit, debit, and other payment cards provided through General Services Administration (GSA) contracts have enhanced security features, and shall begin replacing credit, debit, and other payment cards without enhanced security features no later than January 1, 2015.**

(c) The Secretary of the Treasury shall **take necessary steps to ensure that Direct Express prepaid debit cards for administering Government benefits have enhanced security features**, and by January 1, 2015, the Department of the Treasury shall **develop a plan for the replacement of Direct Express prepaid debit cards without enhanced security features.**

(d) By January 1, 2015, other agencies with credit, debit, and other payment card programs shall provide to the Office of Management and Budget (OMB) plans for ensuring that their credit, debit, and other payment cards have enhanced security features.

54. By early 2018, 91% of all U.S. ATMs had converted to EMV-enabled ATM terminals to service EMV-enabled debit and credit cards.⁶⁸ By March 2019, 99% of Visa's U.S. payments volume (\$81B) was completed using an EMV chip card.⁶⁹

55. In my opinion, based on the above facts and my experience, by at least 2019, EMV had become the industry standard for payment card security in the United States.

⁶⁸ Nearly All US ATMs Now EMV-Capable, Study Finds, ATM Marketplace (April 6, 2018), <https://www.atmmarketplace.com/news/nearly-all-us-atms-now-emv-capable-study-finds/>.

⁶⁹ See Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent, VISA (May 28, 2019, 3:28 PM), <https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html>; EMV in the U.S. (2020 Update), Thales (2020), <https://www.thalesgroup.com/en/americas/united-states/digital-identity-and-security/emv>; see also Understanding the U.S. EMV Liability Shifts, US Payments Forum at 4 (July 2017), <https://www.uspaymentsforum.org/wp-content/uploads/2017/07/EMV-Fraud-Liability-Shift-WP-FINAL-July-2017.pdf>.

D. The Bank's Failure to Include EMV Chips in its EDD Debit Cards Resulted in Cards with Below Industry Standard Security.

56. The Bank promised in its contract with EDD to “employ the highest level of security and fraud safeguards” for EDD debit cardholders.⁷⁰ However, for many years after the Bank had converted its consumer and commercial debit cards to EMV chip cards,⁷¹ and even after 2019 when the U.S. market reached the milestone with 99% of U.S. payments volume being processed as EMV within the U.S.,⁷² the Bank continued to issue mag-stripe only cards to its EDD debit cardholders and did not provide EDD debit cardholders the same level of security it afforded to its commercial customers.⁷³

57. By failing to include EMV chips in its EDD debit cards in the beginning of 2020, the Bank did not provide EDD debit cardholders the “highest level of security and fraud safeguards.”⁷⁴ As described in paragraphs 36-45 and the paragraphs below, by 2019 EMV technology was the industry standard for all credit and debit cards issued in the United States, including for debit cards used in the administration of government benefits. Even though EMV chips are considerably more secure than mag-stripe only cards and better protect the cardholder from card-present counterfeit fraud for the reasons stated above,⁷⁵ the Bank did not include its EDD debit cards in its EMV migration in 2014.⁷⁶ The Bank's failure to include EMV chips in its EDD debit cards thus resulted in cards with below basic industry standard security. For all the

⁷⁰ BANA's Response to State of California Electronic Benefits Payments RFP Vol. I & II at 253-54.

⁷¹ See Martin Tr. 61:19-23 (Bank has included EMV chips in all consumer and small business debit cards issued since late 2014).

⁷² Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent, VISA (May 28, 2019, 3:28 PM), <https://usa.visa.com/visa-everywhere/blog/bdp/2019/05/28/chip-technology-helps-1559068467332.html>.

⁷³ Martin Tr. 65:4-14, 65:8-10.

⁷⁴ BANA's Response to State of California Electronic Benefits Payments RFP Vol. I & II at 253-54.

⁷⁵ See *supra* ¶¶ 29-45.

⁷⁶ Martin Tr. 65:4-14, 65:8-10.

reasons discussed above, the lack of EMV chips in EDD debit cards rendered them highly susceptible to card skimming and card-present counterfeit fraud.⁷⁷

E. The Bank's Decision to Not Include EMV Chips in EDD Debit Cards in Early 2020 Was Inconsistent with Other Participants in the Payments Industry.

58. Documents produced by the Bank in this litigation demonstrate that the Bank knew as early as January 2020 not only that (1) EMV was already the industry standard for debit card security, but also that (2) the cost of making a modest investment in EMV chips for the EDD debit card portfolio would [REDACTED]

[REDACTED].⁷⁸ It is therefore my opinion, based on my industry experience and expertise, that the Bank's decision not to include EMV chips in EDD debit cards at least as of January 2020 was highly inconsistent with how I would expect a sophisticated financial institution in the payments industry to make decisions regarding payment card security.

59. Bank documents suggest that the Bank did not implement EMV in EDD debit cards before 2020, despite the well-established benefits of EMV for cardholders, as described above, due to [REDACTED].⁷⁹

60. By early 2020, however, not only had EMV been the industry standard throughout the credit and debit card market for at least a year,⁸⁰ but the Bank's own internal analyses cited [REDACTED]

⁷⁷ I understand that it was not until July 2021, shortly after a preliminary injunction was issued against Bank in this lawsuit, that the Bank finally begin issuing EMV cards to new EDD debit cardholders and to existing cardholders whose cards needed to be replaced. Martin Tr. 65:8-10.

⁷⁸ See BANA_EDD_MDL-351839 at -351839-40.

⁷⁹ See BANA_EDD_MDL-116001 at -116001 ("[REDACTED]").

⁸⁰ See *supra* ¶¶ 47-56.

61. The Bank acknowledged in a presentation dated January 27, 2020, that

[REDACTED]”⁸¹ Under the Electronic Funds Transfer Act (“EFTA”) and EFTA’s implementing Regulation E, the Bank would be liable for card-present transaction fraud,⁸² and under the liability shift rules, unauthorized card-present transactions on EDD debit card accounts would not be recoverable by the Bank where the transaction took place at an ATM or payment terminal with a chip reader.⁸³

62. As a result, the Bank's own **pre-pandemic** cost-benefit analysis in January 2020, [REDACTED] described below, demonstrated that [REDACTED]

63.

⁸⁴ In turn,

⁸¹ BANA EDD MDL-370150 at -370154 (emphasis added).

⁸² See 15 U.S.C. §1693f(b); 12 C.F.R. §1005.11(c)(1).

⁸³ See *supra* ¶ 50.

⁸⁴ See BANA EDD MDL-351839 at -351839–40. A [REDACTED]
[REDACTED]. See BANA EDD MDL-104742 at -104744.

⁸⁵ BANA EDD MDL-351839 at -351839.

86

From: Smith, Katherine C
Sent: Friday, January 10, 2020 12:14 PM
To: Garfield, Bradley <bradley.garfield@bofa.com>
Subject: EMV Cost Benefit Analysis

(000s)		Jan-20	Feb-20	Mar-20	Apr-20	May-20	Jun-20	Jul-20
CA EDD 2020 Forecast	Value Load	\$1,087,812.04	\$968,820.01	\$1,060,077.71	\$976,080.49	\$916,034.70	\$831,360.96	\$876,302.78
	Rev Share	\$ (596.02)	\$ (591.94)	\$ (532.32)	\$ (568.30)	\$ (521.82)	\$ (504.41)	\$ (459.11)
	Card Issuance	126	112	123	113	106	96	102
	Total EMV Card Issuance Cost	\$ 185.94	\$ 165.61	\$ 181.20	\$ 166.85	\$ 156.58	\$ 142.11	\$ 149.79
	Incremental EMV Card Issuance Cost	\$ 49.61	\$ 44.18	\$ 48.35	\$ 44.51	\$ 41.78	\$ 37.91	\$ 39.96
	Fraud Savings	\$ 122.13	\$ 108.77	\$ 119.02	\$ 109.59	\$ 102.85	\$ 93.34	\$ 98.39
	Net Fraud Savings	\$ 72.52	\$ 64.59	\$ 70.68	\$ 65.07	\$ 61.07	\$ 55.43	\$ 58.42

Aug-20	Sep-20	Oct-20	Nov-20	Dec-20	Total
\$818,338.37	\$803,952.29	\$912,911.81	\$858,440.72	\$955,475.26	\$11,065,607.15
\$ (454.18)	\$ (437.35)	\$ (410.35)	\$ (422.21)	\$ (402.81)	\$ (5,900.82)
95	93	106	100	111	1,284
\$ 139.88	\$ 137.42	\$ 156.05	\$ 146.74	\$ 163.32	\$ 1,891.50
\$ 37.32	\$ 36.66	\$ 41.63	\$ 39.15	\$ 43.58	\$ 504.66
\$ 91.88	\$ 90.26	\$ 102.50	\$ 96.38	\$ 107.28	\$ 1,242.40
\$ 54.56	\$ 53.60	\$ 60.86	\$ 57.23	\$ 63.70	\$ 737.74

64. The head of the Bank's EDD debit card product team, Brad Garfield, noted that

„⁸⁷ Garfield explained in an email dated January 10, 2020: “

„⁸⁸

65. Prior to the pandemic, the Bank's business case alone, regardless of past practice, should have been clear as to the need to convert EDD debit cards to EMV technology. The Bank recognized that (1)

⁸⁶ *Id.*

⁸⁷ *Id.* Garfield leads card products within the Bank's Global Transactions Services group. *See* BANA_EDD_MDL-57837 at -57850.

⁸⁸ *Id.* (emphasis added).

91

66. Despite

[REDACTED], the Bank continued to ignore industry standards and its cardholder's interests by deciding not to include the higher security EMV chips in its EDD debit cards. In my experience working in EMV transitions across multiple markets, products, and stakeholders, I have never observed an institution make a similar decision to forego an option that its own analysis [REDACTED]

67. I have known many industry stakeholders to make investments in EMV on far weaker business cases than the Bank had here, relying instead on a combination of both quantitative factors (costs and benefits of investment dollars) and qualitative factors (such as customer experience, ubiquity of acceptance, and trust built on network reliability and security). In my experience, for many markets, the quantitative analysis predicted 4 or more years to break even and 6-7 years to reach a positive net present value. Yet those markets moved forward with conversion to EMV on the strength of the qualitative components. Here, the Bank's analysis showed

Given this analysis, the Bank's failure to convert its EDD debit cards to EMV chip cards was highly irregular compared to the behavior of other participants in the payments sector.

⁸⁹ See BANA EDD MDL-351839 at -351839 (

⁹⁰ *Id.* at -351839-40.

⁹¹ *Id.* at -351839.

68. Documents produced by the Bank in this litigation indicate that the Bank

69. The contract between the Bank and EDD provided that the parties would split the revenue earned on “float,” i.e. interest earned on EDD debit cardholders’ account balances.⁹³ As indicated in internal emails exchanged among Bank officials, the Bank [REDACTED]

As one internal Bank email explained:

70. Another internal email from Brad Garfield, head of the Bank's EDD debit card product team, dated March 10, 2020 also explained [REDACTED]

⁹² See BANA_EDD_MDL-351839 at -351839-40; BANA_EDD_MDL-102937 at -102937; BANA_EDD_MDL-116001 at -116001; BANA_EDD_MDL-123235 at -123235.

⁹³ Chestnut Tr. 55:21-56:9, 169:1-170:13.

⁹⁴ BANA EDD MDL-116001 at -116001; *see also* BANA EDD MDL-102937 at -102937

.”); BANA EDD MDL-352396 at -352396

71. In an email dated February 25, 2020, Garfield laid out the Bank's

⁹⁵ BANA_EDD_MDL-351839 at -351839 (emphasis added).

[REDACTED]

[REDACTED]

[REDACTED]

72. In March 2020, the Bank created a PowerPoint document entitled “[REDACTED]

[REDACTED]⁹⁷ [REDACTED]

[REDACTED]⁹⁸ [REDACTED]

[REDACTED].”⁹⁹ All of those facts and observations are accurate, based on my personal, expert knowledge and experience, and consistent with the industry reports cited above.¹⁰⁰

73. [REDACTED]

⁹⁶ BANA_EDD_MDL-123235 at -123235 (emphasis added).

⁹⁷ BANA_EDD_MDL-167019 at -167019–24.

⁹⁸ *Id.* at -167021.

⁹⁹ *Id.* at -167021.

¹⁰⁰ *See supra* ¶¶ 29-45, n.30-51.

Response	Percentage
Yes, the current government is responsible	100%
No, the current government is not responsible	0%
Don't know	0%

74. Despite the Bank's

[REDACTED]
[REDACTED]
[REDACTED], it is my understanding that [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

¹⁰¹ BANA_EDD_MD L-167019 at -167022 (emphasis added).

102 *Id.*

103 *Id.*

¹⁰⁴ Martin Tr. 65:8-10.

75. Based on my review of these Bank documents and my expertise, it is clear that, before the onset of the pandemic, the Bank understood that [REDACTED], and that the Bank was aware of [REDACTED]. It is also clear that the Bank had determined as of January 2020 that [REDACTED]. Given these factors, in my extensive experience building and analyzing business cases for EMV chip migration, I would have recommended and expected the Bank to migrate the EDD portfolio to EDD no later than January 2020. The Bank's decision not to make a minor investment [REDACTED], which would have sharply reduced the increasing fraud losses the Bank was experiencing and provided industry standard card security to cardholders, evidently because the [REDACTED], was highly irregular and, in my opinion, irresponsible to EDD cardholders.

76. Even after witnessing historic fraud on EDD debit cards in 2020 during the COVID-19 pandemic, the Bank still did not act swiftly to add EMV chips to EDD debit cards. An Executive Summary on the prepaid unemployment card portfolio presented by the Bank sometime in mid-to-late 2020 suggests that [REDACTED]

.¹⁰⁵

¹⁰⁵ BANA_EDD_MDL-104742 at -104744, -104746.

77. Yet still the Bank did not begin issuing EMV chip cards to new EDD debit cardholders and to existing cardholders whose cards needed to be replaced until July 2021, shortly after a preliminary injunction was issued against Bank in this lawsuit.¹⁰⁶

78. The Bank's failure to meet industry standards for fraud security before July 2021 was particularly egregious, in my opinion, because (1) EMV was industry standard at least a year before the pandemic; (2) months before the pandemic began, the Bank had [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]; and, finally, (3) the Bank was aware of the ability of EMV to prevent the fraud cardholders were experiencing throughout the pandemic. Yet instead of immediately implementing a switch to EMV at any of those points, the Bank did not begin conversion until July 2021, thus exposing every EDD debit cardholder to the risk of card-present counterfeit fraud for no justifiable reason.

F. It Was Highly Foreseeable that the Bank's Failure to Include EMV Chips in EDD Debit Cards Would Lead to Counterfeit Fraud Targeting EDD Debit Cardholders During the Pandemic, Because Fraud Migrates to the Weakest Link.

79. It is well established that fraud migrates to the weakest link. As described in examples below, long before the pandemic, industry experts had warned that retailers and banks that lagged in implementing EMV after the liability shift risked increasing their cardholders' vulnerability to fraud. Indeed, experts had long been raising warnings to smaller programs and merchants that there was significant risk to further delaying EMV chip implementation.

80. The 2016 Community Banking Connection report, a nationwide Federal Reserve System resource for community banks, identified the risk smaller programs faced related to

¹⁰⁶ Martin Tr. 65:8-10.

becoming the “easiest target” for criminals:¹⁰⁷

What is the risk of delaying? Timing is another factor to consider. **Migration to chip cards is a version of “musical chairs” for card issuers: No one wants to be the last one in a market to convert to chip cards because fraudsters tend to attack the easiest targets first.** Because magnetic stripe cards are easier to counterfeit, they are generally attractive targets for thieves.

81. In June 2017, the American Banker similarly warned in an article entitled, “Crooks Are on the Prowl for Late EMV Converts,” that smaller banks are at risk of being “in the cross hairs of criminals poised to exploit obvious holes” and may face a major fraud event:¹⁰⁸

More than 60% of all U.S. payment cards are now EMV-enabled and just over half of all merchants are chip-compliant, which has slashed counterfeit card risk for many operators. But the U.S. has a long way to go before full conversion to the EMV standard is completely finished, and **those who delay may find themselves in the cross-hairs of criminals poised to exploit obvious holes in the system.** Smaller financial institutions and merchants in specific categories that have not made the move to EMV **may now be at higher risk for counterfeit card losses from criminals exploiting account data on the shrinking number of older magnetic-stripe payment cards not yet equipped with the more secure EMV chip technology.**

A handful of smaller banks still haven’t taken action on EMV, and **they may have to get hit by a significant fraud event before they’re convinced they need to invest the money and time into finally converting to chip cards,** “says Troy Bernard, director of strategic marketing and products at CPI Card Group, a card manufacturer.

¹⁰⁷ Mary J. Hughes, The U.S. EMV Chip Card Migration: Considerations for Card Issuers, Community Banking Connections (2016), <https://www.communitybankingconnections.org/articles/2016/i1/emv-chip-card-migration> (emphasis added).

¹⁰⁸ Kate Fitzgerald, Crooks Are On the Prowl for Late EMV Converts, American Banker (Jun 23, 2017, 12:01 AM), <https://www.americanbanker.com/payments/news/crooks-are-on-the-prowl-for-late-emv-converts> (emphasis added).

82. In April 2018, Javelin Research reported that criminals were beginning to focus on mag-stripe only debit and prepaid cards, with counterfeit fraud targeting prepaid cards nearly tripling compared to the previous year:¹⁰⁹

Transaction fraud losses are falling because of EMV and a shift in behavior. As more and more credit cards are meeting the EMV standard, **criminals are focusing their attention on less lucrative debit and prepaid cards. In 2017, roughly 3.4 million people lost control of their prepaid cards — nearly three times as many as the previous year.** The average amount per fraudulent transaction is declining. In the same period, debit card fraud victims rose from 5.2 million to 6.6 million.

83. Thus, even before the start of the pandemic, the industry was warning that the lack of EMV chips cards made mag-stripe only debit and prepaid cards targets for skimming attacks and counterfeit card fraud.

84. In addition, the pre-pandemic load values (a term for the amount of money being added to or “loaded” onto the benefit cards) for the EDD program were already large enough to be an attractive target for counterfeiting.¹¹⁰ The sheer volume of money that the Bank was administering provided an incentive for criminals to target the program.

85. Based on my experience, a sophisticated financial institution like Bank of America would have been aware well before the start of the pandemic of the high risk that fraudsters would target its EDD debit cardholders because their mag-stripe only cards were particularly vulnerable to skimming and counterfeit fraud. Indeed, a Bank presentation dated January 27, 2020 confirms the Bank’s awareness that its EDD debit cards had become an attractive target for fraud:

[REDACTED]

¹⁰⁹ From Application to Transaction: Card Fraud Trends, Threats, & Tactics at 5 (April 2018), <https://javelinstrategy.com/sites/default/files/files/reports/18-5006J-FM-From%20Application%20to%20Transaction-FIS.pdf> (emphasis added).

¹¹⁰ See BANA EDD MDL-154042 at -154042 [REDACTED]

[REDACTED]

86. The impact of the pandemic increased both the number of benefit recipients and the total load value on EDD debit cards, which were reloaded with benefits every two weeks.¹¹² This made the vulnerabilities in the Bank's administration of the EDD program even more attractive to criminals.¹¹³ Based on my experience, it would have been foreseeable to any sophisticated financial institution like Bank of America at the onset of the pandemic that the increase in EDD debit card load, combined with the known security vulnerabilities of mag-stripe-only EDD debit cards, would make EDD debit cards an even more attractive target for card skimming and counterfeit fraud during the pandemic, in the absence of EMV chip cards.

87. Indeed, several documents produced by the Bank in discovery (1) demonstrate the

[REDACTED]

[REDACTED] (2) confirm [REDACTED]

[REDACTED] and (3) demonstrate the

[REDACTED]

[REDACTED].

¹¹¹ BANA_EDD_MDL-370150 at -370154 (emphasis added).

¹¹² BANA_EDD_MDL-059687 at -59687-88 ([REDACTED]); BANA_EDD_MDL-154042 at -154042 ([REDACTED]); BANA_EDD_MDL-153666 at -153670 ([REDACTED]).

¹¹³ During the pandemic, reports confirmed that EDD debit cardholders were falling victim to skimming and counterfeit card fraud. For example, on November 13, 2020, NBC Los Angeles identified three victims of likely skimming fraud who had their EDD funds stolen from their accounts. See Christine Roher, Thousands Are Being Stolen From Bank of America Accounts, and EDD May Be Linked. Here's How to Protect Yourself, NBC Los Angeles (Nov. 14, 2020, 3:07 PM), <https://www.nbclosangeles.com/news/local/edd-bank-of-america-fraud-bank-account-stolen/2462198>. On November 20, 2020, CalMatters wrote about five additional victims of skimming fraud related to EDD accounts. Lauren Helper & Stephen Council, How Bank of America Helped Fuel California's Unemployment Meltdown, CalMatters (Nov. 20, 2020), <https://calmatters.org/economy/2020/11/how-bank-of-america-helped-fuel-californias-unemployment-meltdow>.

[illegible]

89. [REDACTED] Another email dated April 23, 2020 similarly confirms that [REDACTED]
[REDACTED] (i.e. non-prepaid debit cards, all of which had EMV chips as of 2014), “[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]”¹¹⁷

90. In an internal email dated May 22, 2020, the Bank acknowledged that “[REDACTED]”
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]”
[REDACTED]

91. In an internal email chain on July 9, 2020, William Martin (current Bank Management Executive for Prepaid Unemployment Programs and former Senior Fraud Policy Manager¹¹⁹) asked: “

¹¹⁴ BANA EDD MDL-228914 at -228914 (emphasis added).

115 *Id.*

¹¹⁶ *Id.* (emphasis added)

¹¹⁷ BANA EDD MDL-297295 at -297295 (emphasis added).

¹¹⁸ BANA EDD MDL-171972 at -171973.

¹¹⁹ Martin Tr. 26:11-25; *see also* BANA EDD MDL-57837 at -57844.

[REDACTED]”¹²⁰
Melody Szretter, who oversaw the Bank’s fraud strategies for EDD prepaid debit cards in the 2020-2021 time period,¹²¹ replied: “[REDACTED]

[REDACTED]”¹²²

92. In another email dated August 18, 2020, Bank employees discussed seeing an “[REDACTED],” explaining that [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]”¹²³

93. In an internal email dated September 9, 2020, Brad Garfield, head of the EDD debit card product team, noted that [REDACTED]
[REDACTED],” and [REDACTED]
[REDACTED]....”¹²⁴

94. The Bank’s documents show that the Bank understood, consistent with my opinion, that adding an EMV chip to its cards would provide the best protection against counterfeit fraud. In an internal email dated November 2, 2020, Melody Szretter, in response to a question from Brad Garfield about [REDACTED]

[REDACTED], wrote: “[REDACTED]
[REDACTED]”¹²⁵

¹²⁰ BANA_EDD_MDL-172469 at -172471–72.

¹²¹ Martin Tr. 37:2-4; *see also* BANA_EDD_MDL-57837 at -57844.

¹²² BANA_EDD_MDL-172469 at -172471–72 (emphasis added).

¹²³ BANA_EDD_MDL-455617 at -455617 (emphasis added).

¹²⁴ BANA_EDD_MDL-154042 at -154043; *see also* BANA_EDD_MDL-370150 at -370154.

¹²⁵ BANA_EDD_MDL-163307 at -163307 (emphasis added).

95. Based on these Bank documents and others, it is evident that the Bank knew its EDD debit card program was highly attractive to criminals given the high dollar amounts pre-pandemic and even higher dollar amounts during the pandemic combined with a lack of EMV chip security, which is consistent with my opinion that EDD debit cards were in fact highly attractive to criminals during the pandemic and highly susceptible to skimming and counterfeit fraud because they lacked industry-standard EMV chips. Had the Bank issued its EDD debit cardholders industry-standard EMV chip cards, just as it had issued its other consumer and small business debit cardholders EMV chip cards since 2014, EDD debit cardholders would have been protected from such fraud. Had the Bank begun its migration of the EDD card portfolio to EMV when the rise in counterfeit fraud became evident in 2019, the Bank would have had EMV chip cards in place before or at the very least early in the pandemic, which would have prevented much of the subsequent loss and hardship that EDD cardholders experienced as a result of skimming and counterfeit fraud. The Bank nonetheless made a deliberate choice not to adopt EMV chips in EDD debit cards for reasons that are wholly inconsistent with my experience of how participants in the payment sector make their EMV migration decisions.

G. The Bank's Decision Not to Issue EMV Chip Cards to EDD Debit Cardholders Led to an Increase in Skimming Attacks Targeting California EDD Cards.

96. In my professional opinion, the most likely explanation for the unauthorized ATM withdrawals class members experienced while their EDD debit cards were still in their possession is the use of a counterfeit card created as a result of skimming.¹²⁶

97. The lack of an EMV chip in a mag-stripe only card renders that card susceptible to skimming and to counterfeit card fraud. The Bank's failure to issue industry-standard EMV chip cards to EDD cardholders subjected all EMV chip class members to an unnecessary and

¹²⁶ This conclusion is bolstered by the narrow definition of the class, which includes only those individuals who reported unauthorized ATM transactions while still in possession of their ATM cards. This immediately excludes as a possibility the use of a lost or stolen card to carry out the transactions class members reported.

heightened risk of unauthorized access to and disclosure of information on their EDD cards and in their EDD debit card accounts—including from skimming and from any subsequent uses of their skimmed information.

98. The Bank’s decision not to equip EDD cards with EMV chips made all EDD cardholders more vulnerable and significantly increased the likelihood that those cardholders would become the victims of having their personal information accessed through skimming.

99. The Bank’s decision not to include EMV chips in the EDD debit cards portfolio, which grew rapidly in load value during the pandemic, foreseeably led to increased skimming attacks targeting EDD cards in California, a predictable increase that the Bank’s own documents demonstrate the Bank was aware of. *See supra* ¶¶ 88-94. Accordingly, the issuance of mag-stripe only EDD cards put each EDD cardholder at much higher risk for unauthorized access and use and disclosure of personal information.

100. This is because mag-stripe only cards, like the EDD debit cards at issue here, are far easier and far more profitable targets of criminal enterprises than EMV chip cards. As stated above, fraud migrates to the weakest link in a system. By 2020, vulnerable mag-stripe only cards like the EDD debit cards that the Bank issued to class members were that “weakest link” in the system. Had the Bank issued EMV chip cards to EDD cardholders, criminals would have had little incentive to target them with skimming attacks. Thus, it was highly foreseeable that the lack of EMV chips on EDD debit cards would lead to increased counterfeit fraud specifically targeting EDD cardholders during the pandemic.

101. This foreseeable outcome of the Bank’s decision not to issue EMV chip cards to EDD cardholders is exactly what happened. In 2020 and 2021, the Bank observed an [REDACTED], specifically.¹²⁷ Again, a Bank employee observed that “[a]s high-value debit and credit cards (where higher card spend justifies higher-cost fraud deterrence) have migrated to EMV technology, fraudster attention has migrated to mag

¹²⁷ BANA EDD MDL-166345 at -166345 (“[REDACTED]”).

stripe-only cards (like EDD), driving up sustained fraud loss rates >50%.¹²⁸ And another Bank employee noted that “fraudsters see our CA ATMs as a jackpot source of vulnerable NON-chip cards.”¹²⁹

102. The Bank’s decision not to issue EMV chip cards thus foreseeably led to an increase in skimming attacks on vulnerable EDD cards, particularly as their load value increased during the pandemic.

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

103. By definition, every class member reported an unauthorized, PIN-enabled ATM withdrawal, which is necessarily a card-present transaction. The inclusion of an EMV chip in EDD debit cards would have prevented all or nearly all of those ATM withdrawals, and to the extent any unauthorized withdrawals could have occurred at non-chip-enabled ATMs, the Bank’s [REDACTED] (which it applied to its non-prepaid consumer cardholders) would have greatly limited the severity of those withdrawals to [REDACTED].

104. As explained, EMV chips are effective at protecting against any unauthorized card-present transactions, particularly at an ATM machine (almost all of which were chip-enabled as of 2020), that a fraudster may attempt with a counterfeit card created using the information stolen from a skimming, data breach, or phishing attack.¹³⁰ See *supra* ¶¶ 29-32, 42-45. Accordingly, EMV would have prevented all or nearly all of the unauthorized ATM transactions that class members experienced.

¹²⁸ BANA_EDD_MDL-370150 at -370154.

¹²⁹ BANA_EDD_MDL-297295 at -297295.

¹³⁰ Although EMV chips would not have prevented unauthorized transactions by family members, which could also be card-present fraud, I am aware of no reason to believe that family fraud constitutes more than a de minimis percentage of the fraud class members experienced.

105. Moreover, had the Bank implemented EMV technology and provided EDD cardholders the same level of card security it provided its non-prepaid consumer cardholders at the time, any attempt to commit fraud on those EMV chip cards through fallback transactions would have been significantly limited by the Bank's own security measures.

106. This is demonstrated by the experience in 2020 of the Bank's non-prepaid debit card portfolio, which contained EMV chips at the time. The Bank [REDACTED]

131

107. [REDACTED], one Bank employee explained:

132

108. The Bank acknowledged

133

109. By 2021, one Bank employee described

134

¹³¹ See, e.g., BANA EDD MDL-228914 at -228914.

132 *Id.*

¹³³ BANA EDD MDL-57504 at -57505.¹³⁴ BANA EDD MDL-431011 at -431012.

110. Thus, in 2020, had the Bank equipped its EDD debit cards with EMV chips and [REDACTED] as it did for its non-prepaid consumer debit cards, any criminal who attempted to use a counterfeit card with a deliberately broken chip at an ATM would have been [REDACTED]

[REDACTED] 135 [REDACTED]

111. The Bank's [REDACTED]

[REDACTED]. The Bank experienced [REDACTED]

[REDACTED] 136 [REDACTED]

112. I am aware of no reason why [REDACTED]

[REDACTED] as it was for the Bank's non-prepaid consumer debit cardholders, had the Bank issued EMV chip cards to EDD cardholders.

113. Had the Bank issued EDD cards with EMV, either the transaction would be declined because no chip was present or the Bank's [REDACTED] would stop or significantly

¹³⁵ There are three types of "CVV numbers" relevant to a payment transaction. The CVV2 that is printed on the back of the card is unrelated to the CVV number written on the mag stripe (described *supra* ¶17) and the iCVV (frequently called dynamic CVV) that can be generated only by an EMV chip. When the Bank requests the cardholder to enter their CVV2 number, it is the number that is printed on the back of the card, as the cardholder cannot see either of the other two. This step provides assurance that the card is in the cardholder's possession. *See* Mitigating Fraud Risk Through Card Data Verification, Visa Business News (Oct. 8, 2015), <https://www.cba-ok.org/wp-content/uploads/2016/09/VBN-Mitigating-Fraud-Risk-Through-Card-Data-Verification-002.pdf>.

¹³⁶ BANA EDD MDL-297295 at -297295 ("[REDACTED]"). My understanding is that "[REDACTED]" refers to the Bank's non-prepaid consumer debit cards, all of which had EMV chips as of 2014. Business Wire, Bank of America Begins Rollout of Chip Debit Cards (Sept. 30, 2014, 11:10 AM), <https://www.businesswire.com/news/home/20140930005292/en/Bank-of-America-Begins-Rollout-of-Chip-Debit-Cards>.

limit the transaction. EMV would have prevented all or nearly all the card-present transaction fraud that class members experienced.

I. Any Financial Institution in the Bank's Situation Would Have Known that Many EDD Cardholders Who Reported Unauthorized PIN-Enabled ATM Withdrawals Were True Victims of Counterfeit Fraud.

114. Plaintiffs' Counsel have informed me that from September 28, 2020 until the preliminary injunction in this case went into effect on June 8, 2021, the Bank ran all incoming EDD debit cardholder unauthorized-transaction claims through its "Claim Fraud Filter" ("CFF") and used the results of that CFF as a basis for automatically denying certain categories of claims (and, for a period of time, for automatically freezing the cardholders' EDD debit card accounts). The Bank's CFF Indicator 1 applied to all "[REDACTED] [REDACTED]," which the Bank interpreted as any claim involving an unauthorized ATM withdrawal.¹³⁷ If a claim involved a claim of an unauthorized ATM withdrawal (which was necessarily a PIN-enabled ATM withdrawal because all ATMs require the use of a PIN), Indicator 1 of the CFF was triggered, and the claim was denied on that basis.¹³⁸ Plaintiffs' Counsel have also informed me that on or about September 28, 2020, the Bank applied its CFF retroactively to claims that had been submitted between April 1, 2020 and September 27, 2020 and which the Bank had already resolved by issuing permanent credit.¹³⁹ For all such

¹³⁷ BANA's Verified Responses & Objections to Plaintiffs Fourth Set of Interrogatories (Nos. 28, 30, and exhibits thereto); BANA_EDD MDL 125177 at -125177; BANA_EDD_MDL_100634 at -100649 (describing Indicator 1 as "[REDACTED]"); Martin Tr. 125:18-126:8, 127:8-10 (similar); Rule 30(b)(6) Depo. of Shane Daniels ("Daniels Tr.") 285:22-286:13, 289:7-12 (similar). Indicator 1 was also [REDACTED]
[REDACTED]). Rule 30(b)(6) Depo. of Michael Letson ("Letson Tr.") 92:15-94:5 (agreeing that [REDACTED]);
[REDACTED]); Daniels Tr. 285:25-286:25; see BANA_EDD MDL 592324 at -592328 (describing Indicator 1 as "[REDACTED]"); BANA_EDD_MDL_090640 at -90640, -90643 (same).

138 *Id.*

¹³⁹ Martin Tr. 175:10-14, 178:13-23; Daniels Tr. 234:24-236:5.

claims that triggered Indicator 1 of the CFF because they had involved a claim of an unauthorized ATM withdrawal, the Bank rescinded the permanent credit that the Bank had previously issued.¹⁴⁰

115. For the reasons explained above, it has long been known throughout the payment services industry that mag-stripe only cards are vulnerable to skimming and card-present counterfeit fraud. Given that knowledge, and based on the Bank's own documents discussed above, it is my opinion that, as a matter of industry practice, it was clear at the time the CFF was in place that due to the absence of EMV chips in the Bank's EDD debit cards, legitimate cardholders were vulnerable to skimming attacks and counterfeiting. It would also have been clear to industry practitioners that criminals could easily create counterfeit cards (using cardholder information obtained either through skimming, phishing, data breaches, or other security attacks) and that, due to the lack of EMV chips in the Bank's EDD debit cards, the criminals could use those counterfeit cards to make unauthorized POS transactions and ATM withdrawals.

116. The Bank's cardholder agreement advised cardholders that they "may incur no liability for unauthorized use of [a] Card" but only "provided [the cardholder] notify [the Bank] within a reasonable time of the . . . unauthorized use."¹⁴¹

117. Industry leaders also knew that innocent cardholders can be the victims of fraud. Visa, Bank of America's card network partner, knows that consumers can be innocent victims. Visa's Zero Liability Policy is designed to protect consumers from fraudulent activity on their cards. Visa explains its Zero Liability Policy to consumers on its website, as specifically protecting fraudulent use of cards offline (meaning card present transactions):¹⁴²

¹⁴⁰ *See id.*

¹⁴¹ BANA_EDD_MDL_536398 at -536402.

¹⁴² With Zero Liability, You're Not Responsible for Unauthorized Charges, Visa, <https://usa.visa.com/pay-with-visa/visa-chip-technology-consumers/zero-liability-policy.html> (last accessed Aug. 9, 2024) (emphasis added).

Visa's Zero Liability Policy* is our guarantee that you won't be held responsible for unauthorized charges made with your account or account information. You're protected if your Visa credit or debit card is lost, stolen or **fraudulently used, online or offline.**

118. The Consumer Financial Protection Bureau, known as CFPB, similarly recognizes that legitimate cardholders can be innocent victims of fraud and provides consumers with advice regarding their protections under law. The CFPB is the federal agency charged with overseeing the financial services industry and protecting consumers from unfair, deceptive, or abusive practices. The CFPB's website poses several Frequently Asked Questions, including one focused on unauthorized transactions on a debit card, which is shown below:¹⁴³

If the unauthorized transaction was made using a debit card or other electronic fund transfer, you might have additional protections under federal law. Electronic fund transfers include ATM transactions, purchases using your debit card, some online bill payments, and payments you've set up to be deducted from your account automatically

What if someone charges my account but I have my physical debit card?

If an unauthorized withdrawal appears on your bank statement, but you did not lose your card, security code, or PIN or had any of them stolen, you should notify your bank or credit union right away.

119. In light of everything discussed above, it is my opinion that any financial institution in the Bank's situation would have known, and the Bank knew or should have known, that many of its EDD debit cardholders who reported an unauthorized ATM withdrawal between April 1, 2020 and June 8, 2021 were in fact victims of counterfeit card fraud that likely resulted from card skimming. The Bank's decision to issue mag-stripe only rather than EMV chip cards to its EDD debit cardholders prior to July 2021 enabled such fraud. It is also my opinion that any financial institution in the Bank's situation would have known, and the Bank knew or should have known, that its "Claim Fraud Filter" strategy would result in the wrongful denial of a

¹⁴³ How Do I Get My Money Back After I Discover an Unauthorized Transaction or Money Missing From My Bank Account, Consumer Financial Protection Bureau (Aug. 28, 2023), <https://www.consumerfinance.gov/ask-cfpb/how-do-i-get-my-money-back-after-i-discover-an-unauthorized-transaction-or-money-missing-from-my-bank-account-en-1017/> (last accessed Aug. 9, 2024).

substantial number of valid claims and the wrongful freezing of accounts of innocent EDD debit cardholders.

VII. CONCLUSION

120. It is my opinion that, from January 2020 to July 2021, Bank of America denied its EDD debit card customers the industry-standard security it had long provided to its commercial debit and credit card customers. Financial institutions knew, as the Bank confirmed in its own words, that including EMV chips on its credit and debit cards would be the most effective tool for fighting counterfeit fraud in a card-present environment. In the years before the pandemic, it was widely recognized and readily foreseeable to everyone in the industry, including the Bank, that fraud would move to the remaining less secure mag-stripe only cards that remained in the market and that card programs that did not convert to EMV would be increasingly targeted by counterfeit fraud.

121. In my professional experience, the Bank's decision to proceed without EMV chips in its EDD debit cards from January 2020 until July 2021, even after [REDACTED]

[REDACTED]

[REDACTED]

was highly irregular in the payments industry.

122. The Bank's failure to issue EMV chip cards to EDD debit cardholders rendered EDD debit cardholders particularly vulnerable to counterfeit card fraud (such as unauthorized ATM withdrawals) that could have been prevented by the presence of an EMV chip on their debit cards.

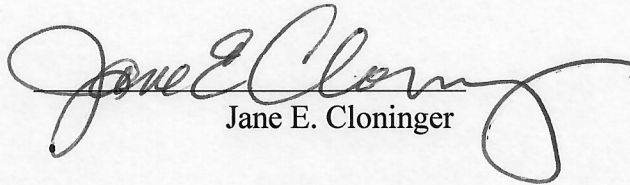
123. As a foreseeable result of the Bank's decision not to introduce industry-standard security EMV chips into EDD debit cards, there was significant card-present transaction fraud targeting the Bank's EDD debit card portfolio during the pandemic, including unauthorized ATM withdrawals).

124. In my opinion any financial institution in the Bank's situation would have known, and the Bank did know or should have known, that due to Bank's decision to issue vulnerable mag-stripe only rather than EMV chip cards to its EDD debit cardholders prior to July 2021, many of its EDD debit cardholders who reported an unauthorized ATM withdrawal between April 1, 2020 and June 8, 2021 were in fact victims of card-present counterfeit fraud that likely resulted from card skimming. It is also my opinion that any financial institution in the Bank's situation would have known, and that the Bank did know or should have known, that its "Claim Fraud Filter" strategy would result in the wrongful denial of a substantial number of valid claims and the wrongful freezing of accounts of innocent EDD debit cardholders.

* * *

* * *

Dated: March 4, 2025


Jane E. Cloninger

Appendix A: Curriculum Vitae

Appendix B: List of Materials Considered

APPENDIX A

JANE E. CLONINGER

San Francisco, CA | jane.cloninger@gmail.com | 415.218.7417 | linkedin.com/in/janecloninger

A senior leader with broad consulting experience in competitive strategy, new product development, business case development and implementation execution. Primary expertise is electronic payments systems, particularly emerging products and technologies including mobile, contactless and EMV for both face to face and online payments and real time payments. Worked in many parts of the card industry including working with card brands, issuers, merchants, co-brand partners, third party processors, and major merchant acquirers. Global experience includes Canada, Latin America, UK, and Australia.

1. EDUCATION

University of California at Los Angeles, Anderson Graduate School of Management, Los Angeles, CA; Master of Business Administration, Strategy and Finance, 1982

University of Tennessee, Knoxville, TN; Bachelor of Science, Economics, 1978 (with honors)

2. EMPLOYMENT HISTORY

Accenture, Senior Managing Director, Accenture Payment Services San Francisco, CA	2017 – 2019
Edgar, Dunn & Company, Director/Partner San Francisco	1985 – 2017
First Interstate Bancorp, Assistant Vice President Los Angeles, CA	1982 – 1985
Wilshire Associates Los Angeles, CA	1979 – 1980

3. SELECTED LITIGATION SUPPORT EXPERIENCE

Jane has provided expert reports and testimony at depositions, mediation, arbitration, and jury trials. Selected examples include the following:

Class Size – Analyzed the likelihood that customers who could potentially benefit from the settlement would have remained customers and that they would have active credit cards on file by which they could receive any settlement funds.

Bankruptcy Dispute – Provided expert opinion and testified in deposition in a case involving the bankruptcy of a charter airline. Provided testimony regarding industry risk management practices and the role and responsibility of the acquirer in underwriting and monitoring their merchant clients.

Securities Litigation – Class Action. In support of a class action lawsuit alleging inappropriate public disclosure of credit card portfolio performance to investors, prepared expert report based on analysis of portfolio performance during each quarter of the class period to determine what actual performance was compared to reported performance. Evaluated loan loss reserves and calculated appropriate reserve levels based on risk exhibited by the portfolio performance indicators. Testified for mediation and prepared Expert Report for settlement purposes. Case settled in favor of our client.

Contract Dispute – Valuation of Co-Brand Credit Card Portfolio. Prepared the damage assessment related to litigation resulting from the co-brand partner's refusal to honor an established co-brand agreement. Assessed the competitive environment and management practices during the interim period to identify any changes in value related to other factors. Provided expert witness testimony in deposition and in a jury trial that concluded in favor of damages for our client.

Contract Dispute – Credit Card Program Valuation. Provided expert witness testimony related dispute between a bank and its former cobrand marketing partner. Developed estimated future earnings potential and loss forecasts to estimate the probable profitability if the program had been continued

4. OTHER SELECTED PROJECT EXPERIENCE

Jane has been a consultant to the credit card and payments industry since 1985. Below are selected examples of projects:

De Novo Digital Bank. Responsible for the client relationship and oversight of various client engagement teams involved in the implementation of a new core banking platform, accounting platform, AML tools and data strategy development.

Business Case Development for Chip. Developed the business case for the migration of a national PIN debit scheme from magnetic stripe technology to chip. Developed the industry business cases for migration within the US considering the costs and benefits to issuers, acquirers/merchants, and processors. Developed the business case for a large regional issuer which included its retail credit and debit programs as well as commercial and prepaid portfolios.

Risk Assessment. Led a review how risk was introduced into a global payment services' core services and how the client identified and responded to incidents. Scope included working with Treasury and Settlement to develop an end-to-end view of the process. Areas addressed including client on-boarding, transaction authorization processing and backend monitoring and settlement. Documented key workflows and made recommendations to address areas of risk including upstream Treasury dependencies.

Payments Roadmap. Developed a payments roadmap for a large transportation company. Identified and prioritized over 20 opportunities for near term and long-term implementation based on their ability to meet management's objectives.

Payment Strategy. Developed the corporate strategy for a national debit brand. Identified what areas of investment to pursue and what not to pursue. Reviewed the competitive landscape to identify threats and opportunities. Assisted client in assessing the impact of changing regulatory and competitive environment on their business. Developed planning scenarios and related volume projections. Identified various competitive and regulatory scenarios and likely merchant and consumer reactions under each scenario. Identified the implications to the client and likely transaction volumes that would result under each competitive scenario.

Product Strategy. Created a Product Roadmap for a national debit brand that outlines the planned product evolution, including opportunities and investment requirements across eleven proposed products, including: contactless, mobile, P2P, cross border debit, bill payment, prepaid and online payments. Assessed the competitive environment, market need, strategic fit, and level of effort and investment required to implement.

Mobile Payments. Developed an NFC commercialization roadmap for a global payment brand. Analysis included identifying key requirements for commercialization and assessing six markets' readiness against those requirements.

5. SELECTED SPEAKING ENGAGEMENTS

- Card Not Present Expo, Moderator, “Remote Control: Focusing on mobile Web and in-app capability vs. mPOS”, May 2016
- Money 20/20, Moderator “Payment Card Innovation – and the Evolving Role of Issuers, Processors and Networks”, October 27, 2015
- ARC Travel Connect, 2015 (Airlines Reporting Company), Speaker and Panel Moderator, “How Do New Developments in Payments Impact the Travel Industry”, Washington DC, October 22, 2015
- Mobile World Congress, Barcelona. Moderator “Mobile Retail: Delivering Contextual Experiences to Drive Loyalty and Spend”, March 16, 2015
- Money 20/20, Moderator “Payment Security Evolution: EMV, Mobile, CNP & Beyond”, November 3, 2014
- Cartes America, “Mobile Payment Ecosystem Views”, May 13, 2014
- Payments Summit, Smart Card Alliance, Mobile Payments, the Battle of the Approaches, February 3, 2014
- Law Seminars International, Palo Alto, CA, “Mobile Payments, Players, and The Customer Experience – and the Issues They Raise, November 21, 2013
- Money 20/20, Panel Moderator “The Future of the Secure Element and Trusted Execution Environment”, October 7, 2013
- Merchant Risk Council, Webinar, May 23, 2013. Results of survey conducted by EDC and MRC: “Mobile Commerce and the Merchant Experience”
- Law Seminars International, San Francisco, CA, November 15, 2013. “Mobile Payments Ecosystem”
- Law Seminars International, Seattle WA, May 13, 2013. “Mobile Payments: Players and Their Technologies”
- Cartes America, Las Vegas, April 23, 2013. “EMV, NFC and Mobile Implementations Based on the US Business Case”
- Merchant Risk Council, Las Vegas, March 28, 2013. Mobile Super Session. “Mobile Commerce”
- Smart Card Alliance, Las Vegas, February 4, 2013. Moderator: “Keynote Plenary Panel Session: The Pressing Issues on EMV Migrations”

6. PUBLICATIONS

2016 Advanced Payments Report, Edgar, Dunn & Company and Cards & Payments Mobile
2015 Advanced Payments Report, Edgar, Dunn & Company and Cards & Payments Mobile
2014 Advanced Payments Report, Edgar, Dunn & Company and Cards & Payments Mobile
2013 Advanced Payments Report, Edgar, Dunn & Company and Cards & Payments Mobile

APPENDIX B

Appendix B: List of Additional Materials Considered

Date	Document Type	Title/Description	Bates Range
2/8/2024	Transcript	Excerpts from the transcript of Plaintiffs' deposition of the Bank's Rule 30(b)(6) designee, Robert Chestnut, taken on February 8, 2024 ("Chestnut Tr.")	
2/14/2024	Transcript	Excerpts from the transcript of Plaintiffs' deposition of the Bank's Rule 30(b)(6) designee, William ("Matt") Martin, taken on February 14, 2024 ("Martin Tr.")	
2/6/2024	Transcript	Excerpts from the transcript of Plaintiffs' deposition of Defendant Bank of America, N.A.'s (the "Bank") Rule 30(b)(6) designee, Shane Daniels, taken on February 6, 2024 ("Daniels Tr.")	
2/16/2024	Transcript	Excerpts from the transcript of Plaintiffs' deposition of the Bank's Rule 30(b)(6) designee, Michael Letson, taken on February 16, 2024 ("Letson Tr.")	
8/7/2024	Article	"The Magnetic Stripe"	
8/12/2021	Article	"Swiping Left on Magnetic Stripes"	
5/30/2012	Article	"The Long Life and Imminent Death of the Mag-Stripe Card"	
9/17/2018	Article	"Why U.S. Counterfeit Credit Card Fraud Is Down 75%"	
7/14/2011	Article	"Taking a Trip to the ATM, Beware of 'Skimmers'"	
3/15/2018	Article	"How to Detect Skimming Devices on ATM's [sic]"	
3/31/2017	Article	"Why I Always Tug on the ATM"	
4/17/2023	Article	"Understanding Card Skimmers and How to Protect Yourself"	
9/18/2017	Article	"ATM Skimming Gets a Tech Upgrade"	
	Article	"What Is Credit Card Fraud?"	
12/6/2002	Article	"Is Your Credit Card Being Skimmed?"	

12/13/2016	Article	“ATM Fraud: The Evolution of An Epidemic:	
3/29/2017	Article	“FICO Reports a 70 Percent Rise in Debit Cards Compromised at U.S. ATMs and Merchants in 2016”	
8/4/2015	Article	“Global Card Fraud Losses Reach \$16.31 Billion – Will Exceed \$35 Billion in 2020 According to The Nilson Report”	
8/2015	Article	“Card Fraud Losses Reach \$16.31 Billion”	
8/1/2024	Article	“How We Can Help You, Skimming”	
3/18/2020	Article	“The Role of the EMV® Specifications”	
9/2022	Article	“EMV At a Glance”	
11/2014	Article	“A Guide to EMV Chip Technology”	
3/2019	Article	“Debunking EMV Myths”	
12/2016	Article	“EMV Implementation Guidance: Fallback Transactions”	
9/16/2024	Article	“Fraud & Fallback: What You Need to Know About Skimming Attacks”	
11/7/2018	Article	““Fallback” Fraud Declines Significantly as Banks Implement New Policies”	
1/27/2017	Article	“ATM ‘Shimmers’ Target Chip-Based Cards”	
4/2018	Report	“From Application to Transaction: Card Fraud Trends, Threats, and Tactics”	
4/6/2018	Article	“Nearly All US ATMs Now EMV-Capable, Study Finds”	
2018	Article	“2018 ATMIA EMV Migration Survey: Executive Summary (2018)”	
6/1/2020	Article	“US Market Hits 1 Billion EMV Chip Cards Milestone, Payments Cards & Mobile”	
2019	Article	“Fraud the Facts 2019”	
2/25/2016	Article	“With Its EMV Conversion Nearly Complete, Canada’s POS Debit Fraud Falls to New Low”	

9/3/2019	Article	“Visa EMV Chip Cards Help Reduce Counterfeit Fraud by 87 Percent”	
6/23/2019	Article	“The Future of U.S. Fraud in a Post-EMV Environment:	
8/17/2022	Article	“EMV Chip Cards: Everything You Need to Know”	
2/27/2025	Article	“Why EMV?”	
2012	Article	“EMV Compliance in the U.S.”	
4/5/2013	Article	“EMV in the USA: The Story So Far”	
7/2017	Article	“Understanding the U.S. EMV Liability Shifts”	
7/3/2012	Article	“Bank of America Switches to EMV Chip Credit Cards for Consumers”	
12/15/2014	Article	“US Shifts to EMV as Obama and Apple Weigh In”	
9/30/2014	Article	“Bank of America Begins Rollout of Chip Debit Cards”	
8/8/2024	Webpage	“Direct Express, Frequently Asked Questions”	
10/23/2014	Order	Exec. Order No. 13681, 79 F.R. 63491	
5/28/2019	Article	“Chip Technology Helps Reduce Counterfeit Fraud by 76 Percent”	
7/10/2015	Document	Excerpts of BANA’s Response to State of California Electronic Benefits Payments RFP Vol I & II	
1/10/2020	Email	[REDACTED]	BANA_EDD_MDL-351839-35140
7/21/2020	Email	[REDACTED]	BANA_EDD_MDL-116001-116002
1/28/2020	Email and Attachment	[REDACTED]	BANA_EDD_MDL-370150-370155
	Statute	15 U.S.C. §1693f(b); 12 C.F.R. §1005.11(c)(1).	
9/30/2020	Email and Attachment	[REDACTED]	BANA_EDD_MDL-104742-104746
10/20/2023	Document	[REDACTED]	BANA_EDD_MDL-057837-057878

2/21/2020	Email	[REDACTED]	BANA_EDD_MDL-102937
2/26/2020	Email	[REDACTED]	BANA_EDD_MDL-123235-123236
3/3/2020	Email	[REDACTED]	BANA_EDD_MDL-352396-352397
3/13/2020	Email and Attachment	[REDACTED]	BANA_EDD_MDL-167019-167024
2016	Article	"The U.S. EMV Chip Card Migration: Considerations for Card Issuers, Community Banking Connections"	
6/23/2017	Article	"Crooks Are On the Prowl for Late EMV Converts"	
4/2018	Article	"From Application to Transaction: Card Fraud Trends, Threats, & Tactics"	
9/9/2020	Email	[REDACTED]	BANA_EDD_MDL-154042-154044
3/28/2020	Email	[REDACTED]	BANA_EDD_MDL-059687-059690
6/11/2020	Email and Attachment	[REDACTED]	BANA_EDD_MDL-15366-153576
11/14/2020	Article	"Thousands Are Being Stolen From Bank of America Accounts, and EDD May Be Linked. Here's How to Protect Yourself"	
11/20/2020	Article	"How Bank of America Helped Fuel California's Unemployment Meltdown"	
4/24/2020	Email	[REDACTED]	BANA_EDD_MDL-228914-228915
4/23/2021	Email	[REDACTED]	BANA_EDD_MDL-297295
7/10/2020	Email	[REDACTED]	BANA_EDD_MDL-172469-172473
8/18/2020	Email	[REDACTED]	BANA_EDD_MDL-455617-455619
11/2/2020	Email	[REDACTED]	BANA_EDD_MDL-163307-163308
	Document	[REDACTED]	BANA_EDD_MDL-00166345

10/30/2020	Email	[REDACTED]	BANA_EDD_MDL-0057504-57506
2/9/2021	Email	[REDACTED]	BANA_EDD_MDL-00431011-14
10/8/2015	Article	"Mitigating Fraud Risk Through Card Data Verification"	
1/2/2024	Document	[REDACTED]	
9/28/2020	Email	[REDACTED]	BANA_EDD_MDL_125177-125179
10/2020	Document	[REDACTED]	BANA_EDD_MDL_100634-100679
10/9/2020	Document	[REDACTED]	BANA_EDD_MDL_592324-592330
12/29/2020	Email	[REDACTED]	BANA_EDD_MDL_090640-90647
3/1/2018	Document	[REDACTED]	BANA_EDD_MDL_536398-536406
8/9/2024	Webpage	"With Zero Liability, You're Not Responsible for Unauthorized Charges"	
8/28/2023	Webpage	How Do I Get My Money Back After I Discover an Unauthorized Transaction or Money Missing From My Bank Account	