NEAL MANNE (*pro hac vice* forthcoming)
nmanne@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1000 Louisiana, Suite 5100
Houston, Texas 77002-5096
[Tel.] (713) 651-9366
[Fax] (713) 654-6666

DREW D. HANSEN (*pro hac vice* forthcoming)
dhansen@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, Washington 98101-3880
[Tel.] (206) 516-3880
[Fax] (206) 516-3883

Attorneys for Plaintiffs
(Additional Counsel for Plaintiffs
listed below signature line)

SUPREME COURT OF NEW YORK
COUNTY OF NEW YORK

WAL-MART STORES, INC.; SAM'S EAST, INC.; SAM'S WEST, DELAWARE INC.; VUDU, INC.; WAL-MART STORES EAST, LP; WAL-MART STORES ARKANSAS, LLC; WAL-MART LOUISIANA, LLC; WAL-MART STORES TEXAS, LLC; WAL-MART PUERTO RICO, INC.; WAL-MART.COM USA, LLC, Plaintiffs, v. VISA U.S.A. INC., Defendant.	Index No. _____ **REDACTED COMPLAINT FOR DECLARATORY JUDGMENT** (Jury Trial Demanded)

Plaintiffs Wal-Mart Stores, Inc., SAM's East, Inc., SAM's West, Delaware Inc., Vudu, Inc., Wal-Mart Stores East, LP, Wal-Mart Stores Arkansas, LLC, Wal-Mart Louisiana, LLC, Wal-Mart Stores Texas, LLC, Wal-Mart Puerto Rico, Inc., and Wal-Mart.com USA, LLC

(collectively, "Walmart") allege the following claims for relief against Defendant Visa U.S.A. Inc. ("Visa"):

I. INTRODUCTION

1. This dispute concerns whether Visa can inhibit Walmart's ability to route any transaction initiated on a Visa-branded debit card through any network available on the card. REDACTED

2. The parties' dispute exists because Walmart implemented a "chip-and-PIN" protocol for debit card transactions: when consumers presented a debit card with an embedded computer chip for payment, Walmart required consumers to insert their card into a terminal that could read the computer chip (instead of swiping the card's magnetic stripe through a terminal) and then required consumers to enter a Personal Identification Number (PIN) to verify their identities (instead of signing). This chip-and-PIN protocol accords with global best practices for fraud prevention: PIN verification is much more secure than signature verification. It also

enables Walmart to route transactions across PIN debit networks rather than signature debit networks, which saves Walmart (and its customers) money.

3. Visa, however, believes that Walmart should be required to use the more fraud-prone mechanism of signature verification for certain debit card transactions, which in the case of a Visa-branded debit card would route debit card transactions across Visa's debit network rather than competitor networks of Walmart's choosing. REDACTED

II. JURISDICTION AND VENUE

4. This Court has jurisdiction over Visa pursuant to CPLR 201 and 302(a) because Visa transacts business within the State; pursuant to N.Y. Gen. Bus. Oblig. Law § 1304(b) because Visa is a foreign corporation registered to do business in this State; REDACTED

5. Venue is proper in this Court pursuant to CPLR 503(a) and (c) because Visa is a foreign corporation whose principal place of business in New York is New York County. REDACTED

III. THE PARTIES

6. Plaintiff Wal-Mart Stores, Inc. is a Delaware corporation with its principal place of business in Bentonville, Arkansas.

7. Plaintiff SAM's East, Inc. is an Arkansas corporation.

8. Plaintiff SAM's West, Delaware Inc. is an Arkansas corporation.

9. Plaintiff Vudu, Inc. is a Delaware corporation.

10. Plaintiff Wal-Mart Stores East, LP is a Delaware corporation.

11. Plaintiff Wal-Mart Stores Arkansas, LLC is an Arkansas corporation.

12. Plaintiff Wal-Mart Louisiana, LLC is a Delaware corporation.

13. Plaintiff Wal-Mart Stores Texas, LLC is a Delaware corporation.

14. Plaintiff Wal-Mart Puerto Rico, Inc. is a Puerto Rico corporation.

15. Plaintiff Wal-Mart.com USA, LLC is a California corporation.

16. Defendant Visa U.S.A. Inc. is a Delaware corporation with its principal place of business in Foster City, California.

IV. FACTUAL ALLEGATIONS

A. Industry Background

1. Debit Cards and PIN vs. Signature Authentication

17. Debit cards were first introduced in the 1970s to allow consumers to withdraw cash or perform other banking activities at automated teller machines (ATMs). They evolved into a way for consumers to pay for goods and services, and debit has become an increasingly popular form of payment in the United States: although in 2000 there were less than half as many debit card payments as credit card payments; by 2012, there were nearly twice as many debit card payments as credit card payments.[1]

[1] Federal Reserve System, *The 2013 Federal Reserve Payments Study: Recent and Long-Term Trends in the United States, 2000-2012*, at 14-15 (July 2014), *available at* https://www.frbservices.org/files/communications/pdf/general/2013_fed_res_paymt_study_detailed_rpt.pdf

18. Consumers using debit cards usually authenticate their identities in one of two ways: either by entering a personal identification number ("PIN"), as consumers do when they withdraw cash from an ATM, or by signing a paper receipt or an electronic panel at a point-of-sale ("POS") terminal ("signature"). These authentication methods are usually known as "cardholder verification methods" or "CVMs."[2]

19. As noted, bank-owned ATMs use PIN verification exclusively. Walmart is not aware of any ATM that allows customers to use signature verification to withdraw cash.

20. PIN verification is significantly more secure and less prone to fraud than signature verification. Signatures can be forged or copied, and cashiers may forget to check the signature on a receipt or POS terminal to make sure it matches the signature on the back of the card. Cashiers are not trained as handwriting experts, so even if they check the signature there is no guarantee they will spot a forgery. Visa even discourages merchants from asking customers for a form of identification so they can check the signature because, Visa claims, that might "deter the use of a Visa card and result in the loss of a potential sale"; and thus: "Visa believes merchants should not ask for ID as part of their regular card acceptance procedures."[3] And banks issuing cards typically do not collect verified signatures from cardholders or do anything to ensure the signature on the card itself is valid, which means there is no guarantee the transaction is not fraudulent even if even if the signature on the card matches the one on the receipt or POS terminal. For example, a counterfeiter could copy a card, sign on the back, and then use the same signature for a fraudulent purchase—even though the signatures match, it is still a

[2] In the payments industry, the terms "authentication," "verification," and "cardholder verification method" or "CVM" are used essentially interchangeably. Throughout the remainder of this document, Walmart will use the term "verification" but certain quotations include the use of "authentication."

[3] Card Acceptance Guidelines for Visa Merchants, at 33 (2015), *available at* https://usa.visa.com/dam/VCOM/download/merchants/card-acceptance-guidelines-for-merchants.pdf

fraudulent transaction. Between 2004 and 2010, for each year data is available, the fraud rate for debit card transactions verified with a signature ("signature debit") was far higher than the rate for debit card transactions verified by a PIN ("PIN debit"). By 2010, signature debit accounted for 91% of all U.S. debit card fraud, with PIN debit accounting for only 9%.[4] As the Federal Reserve Board summarized the findings of a 2013 study: "Among cards, PIN debit card transactions (including both purchases and ATM withdrawals) had the lowest estimated fraud rates by both number and value in 2012."[5]

21. The method of cardholder verification (signature or PIN) also has significant consequences for how debit card transactions can be routed across networks. Generally speaking, there are two types of debit card networks: PIN debit networks, which evolved from regional ATM networks, and signature debit networks, which evolved from Visa and MasterCard's credit card networks. With few exceptions, the method the cardholder uses to authenticate his or her identity determines the type of network across which the transaction will be routed: if a cardholder enters a PIN to verify his or her identity, then the transaction will be routed across a PIN debit network; if a cardholder uses a signature to verify his or her identity, then the transaction will be routed across a signature debit network. Debit cards typically have the ability for transactions to be routed across multiple networks: usually only one signature network option, and one or (typically) more PIN network options, which means that—as long as merchants are able to require PIN verification—they will be able to route transactions across a PIN debit network instead of being limited to a single signature debit network.

---

[4] Patricia Moloney Figliola, Cong. Research Serv., R43925, *The EMV Chip Card Transition: Background, Status, and Issues for Congress*, at 3-4 & fig. 3 (Nov. 27, 2015), *available at* https://www.fas.org/sgp/crs/misc/R43925.pdf

[5] Federal Reserve System, *Strategies for Improving the U.S. Payment System*, at Appendix 4 (Jan. 26, 2015), *available at* https://fedpaymentsimprovement.org/wp-content/uploads/strategies-improving-us-payment-system.pdf

22. Visa and MasterCard both have their own signature debit networks, operating under the Visa and MasterCard brands. In addition, Visa owns the Interlink PIN debit network and MasterCard owns the Maestro PIN debit network; other PIN debit networks unaffiliated with Visa or MasterCard include Star, Pulse, and NYCE.

23. The network over which a debit card transaction is routed—signature or PIN—determines the fees charged to merchants in connection with that transaction. Historically, the fees charged to merchants (known as "interchange fees") for transactions routed across signature debit networks were higher than the fees for transactions routed across PIN debit networks. For example, according to data collected by the Federal Reserve Board, as of 2009, the average interchange fee for signature debit was 56 cents per transaction, or 1.53% of the transaction amount; the average interchange fee for PIN debit was just 23 cents per transaction or 0.56% of the transaction amount.[6]

24. The Visa and MasterCard signature debit networks were historically (and still are now) the only significant signature debit networks; between them, their networks accounted for essentially all U.S. signature debit transactions and dollar volume in 2009 (Visa had 74.3% of transactions and 72.2% of dollar volume; MasterCard had 25.7% of transactions and 27.8% of dollar volume.[7]) Visa has taken steps to make its signature network the exclusive signature network on its cards: for example, Visa's rules prohibited MasterCard's signature debit network from being offered on the same card as Visa's signature debit network.[8] Visa's efforts at exclusivity were successful: as a paper presented to the Board of Governors of the Federal

[6] Debit Card Interchange Fees and Routing, 75 Fed. Reg. 81,722-01, 81,725 (proposed Dec. 28, 2010).

[7] Steven C. Salop, et al., *Economic Analysis of Debit Card Regulation Under Section 920*, Paper for the Board of Governors of the Federal Reserve System ¶ 35 & Ex. 2 (Oct. 27, 2010), *available at* http://www.federalreserve.gov/newsevents/files/merchants_payment_coalition_meeting_20101102.pdf

[8] *Id.* ¶ 153.

Reserve System in 2010 concluded: "[W]e are unaware of any debit card that bears multiple signature debit networks . . . ."[9]

25. The exclusivity of the Visa signature debit network has significant consequences for transaction routing. When a signature is selected as the cardholder verification method, that selection is nearly always dispositive regarding the network ultimately used to process the transaction—transactions with Visa-branded debit cards in which cardholders authenticate their identities with signatures will be routed across the Visa signature debit network. Therefore, the choice of signature as an authentication method operates as a de facto choice of network for transaction routing purposes, and—if merchants cannot require PIN verification—their routing options on a Visa-branded debit card are limited to only one network because of Visa's exclusivity with signature debit.

26. Interchange fees historically varied among PIN debit networks (the Visa-owned Interlink versus Star, NYCE, Pulse, and others), in part because when merchants have routing choices, the networks must compete for their business. To eliminate such competition, Visa attempted to enforce exclusivity for Interlink, its PIN debit network, just as it had successfully on its signature debit network. As of 2009, approximately 89% of the debit cards with Interlink functionality had no other PIN debit network enabled on the card.[10] Visa's successful efforts to make its own network the exclusive signature debit network on its debit cards and its wholly-owned Interlink network the exclusive PIN debit network on its debit cards allowed Visa to maintain its monopoly in debit. As a 2009 Federal Reserve Board working paper explained: "[P]rice competition appears to have diminished . . . as the largest national PIN debit networks

[9] *Id.* ¶153.

[10] *Id.* Ex. 5.

have increasingly required issuers to sign exclusive agreements under which they become the sole PIN network whose logo appears on an issuer's cards."[11]

2. The Durbin Amendment and Regulation II

27. Visa's attempt to restrict competition and ensure that debit card transactions would be routed over Visa-owned networks through anti-competitive exclusivity arrangements was part of what led Congress to adopt the Durbin Amendment to the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act.[12] The Durbin Amendment prohibits debit card exclusivity and routing priority agreements, instructing the Board of Governors of the Federal Reserve System ("Board") to issue regulations that prohibit issuers and networks from exclusivity agreements (restricting debit networks over which a transaction may be processed to a single network or two or more that are owned by affiliates) (15 U.S.C. § 1693o-2(b)(1)(A)) and ban issuers and networks from "inhibit[ing] the ability of any person who accepts debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions." *Id.* § 1693o-2(b)(1)(B).

28. On December 28, 2010, after a broad-ranging public outreach process that included meetings with debit card issuers, payment card networks, merchant acquirers, merchants, industry trade associations, and consumer groups, as well as a set of surveys distributed to industry participants, the Board offered proposed rules to implement the Durbin Amendment as a new Regulation II: Debit Card Interchange Fees and Routing.[13] In the part most relevant here, the proposed rule imposed a "Prohibition on Routing Restrictions" stating:

[11] Robin A. Prager et al., *Interchange Fees and Payment Card Networks: Economics, Industry Developments, and Policy Issues*, Finance & Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs, Federal Reserve Board, Washington, D.C., at 27 (May 13, 2009) *available at* https://www.federalreserve.gov/pubs/feds/2009/200923/200923pap.pdf

[12] Pub. L. No. 111-203, 124 Stat. 1376 (2010).

[13] Debit Card Interchange Fees and Routing, 75 Fed. Reg. 81,722-01, 81,722-25 (proposed Dec. 28, 2010).

"[A]n issuer or payment card network is prohibited from inhibiting a merchant's ability to route or direct the transaction over any of the payment card networks that the issuer has enabled to process an electronic debit transaction for that particular debit card." The proposed rule identified several examples of issuer or network practices that would be prohibited, including: "Prohibiting a merchant from encouraging or discouraging a cardholder's use of a particular method of debit card authorization, such as rules prohibiting merchants from favoring a cardholder's use of PIN debit over signature debit, or from discouraging the cardholder's use of signature debit."[14]

29. The Board explained that this example "addresses issuer or card network rules or requirements that prohibit a merchant from 'steering,' or encouraging or discouraging, a cardholder's use of a particular method of debit card authorization. For example, merchants may want to encourage cardholders to authorize a debit card transaction by entering their PIN, rather than by providing a signature, if PIN debit carries a lower interchange rate than signature debit. Under [the proposed rule and comment], merchants may not be inhibited from encouraging the use of PIN debit by, for example, setting PIN debit as a default payment method or blocking the use of signature debit altogether."[15]

30. Predictably, as the Board explained, this example drew the opposition of "[a] payment card network and a few issuers," which complained that, "under the proposed example, merchants would be permitted to block a consumer's choice of signature debit."[16] Perhaps not surprisingly, Visa was the "payment card network" that opposed this example: in a submission to

---

[14] *Id.* at 81,763 (emphasis added).

[15] *Id.* at 81,752 (emphasis added).

[16] Debit Card Interchange Fees and Routing, 76 Fed. Reg. 43,394-01, 43,453 (July 20, 2011) (to be codified at 12 C.F.R. pt. 235).

the Board, Visa unsuccessfully argued that because the proposed rule would "expressly permit" a merchant to "block[] the use of signature debit altogether," it was inconsistent with the statutory language: "A contractual term ensuring a customer's right to choose signature debit or PIN does not itself inhibit a merchant's routing choices, rather, the customer's refusal to provide a PIN creates the inhibition, and nothing in the statute forbids a customer from creating such an inhibition."[17] The Board explicitly rejected Visa's argument in its final rule, stating the example was "adopted as proposed." As the Board explained, for a card with a single signature debit network and a single unaffiliated PIN debit network enabled: "[A] merchant can influence routing choice by, for example, determining whether a debit card is PIN-enabled and, if it is, prompting the cardholder to input his or her PIN, rather than asking the consumer whether the transaction is 'debit' or 'credit'." Merchants might want to do this not just because of cost but for fraud prevention. As the Board stated: "[M]erchants may want to encourage cardholders to authorize a debit card transaction by entering their PIN, rather than by providing a signature, because PIN debit carries a lower risk of fraud than signature debit."[18]

31. The final Regulation II language on routing restrictions states: "An issuer or payment card network shall not, directly or through any agent, processor, or licensed member of the network, by contract, requirement, condition, penalty, or otherwise, inhibit the ability of any person that accepts or honors debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions." 12 C.F.R. § 235.7. The Board explained that the practical result of this ban on routing

[17] Visa, Letter to Jennifer J. Johnson, Secretary, Board of Governors of the Federal Reserve System, re Docket No. R-1404 (RIN No. 7100 AD63), Debit Card Interchange Fees and Routing, at 21 (Feb. 22, 2011), *available at* http://www.federalreserve.gov/SECRS/2011/March/20110304/R-1404/R-1404_022211_67810_571316902268_1.pdf

[18] Debit Card Interchange Fees and Routing, 76 Fed. Reg. 43,394-01, 43,453 (July 20, 2011) (to be codified at 12 C.F.R. pt. 235).

restrictions would be that "merchants, not issuers or networks, will be able to direct the routing of transactions."[19] As the Board later stated in its briefing to the D.C. Circuit defending Regulation II, the Board wanted to protect merchants' ability to direct transaction routing, which the Board believed was essential to jump-starting competition, by requiring a particular authentication method. "Steering customers to one authentication method over another—for example, by promoting a consumer to enter his or her PIN rather than signature at the point of sale—is an important way in which merchants facilitate competition between PIN and signature networks."[20] And thus, the Board explained: "[T]he Rule . . . precludes issuer or network practices that prevent merchants from 'steering' consumers to one authentication method over another, by, for example, 'encouraging or discouraging a cardholder's use of a particular method of debit card authorization.'"[21]

3. EMV Chip Cards

32. When Regulation II was issued in 2011, nearly all U.S. cards (both credit and debit) were magnetic stripe cards, with a magnetic stripe on the back of the card that contains cardholder, account, and other information. The next generation of debit and credit cards have an embedded computer chip in addition to a magnetic stripe. The chip contains consumer and account information (like a magnetic stripe) but also has the ability to process information and interact with a POS terminal. The new chip cards are sometimes also called "EMV" cards, after the first letters of the three companies—Europay, MasterCard, and Visa—that initially developed the specifications for the chip technology.

---

[19] *Id.* at 43,452 (emphasis added).

[20] Brief for Defendant-Appellant Board of Governors of the Federal Reserve System at 31 n.3, *NACS v. Bd. of Governors of the Fed. Reserve Sys.*, 746 F.3d 474 (D.C. Cir. 2014) (No. 13-5270)

[21] *Id.* at 30-31 (quoting 12 C.F.R. § 235.7(b), Commentary at cmt. 7(b)(2), *available at* Debit Card Interchange Fees and Routing, 76 Fed. Reg. 43,394-01, 43,475 (July 20, 2011) (to be codified at 12 C.F.R. pt. 235)).

33. Visa set an October 1, 2015 target for U.S. banks to issue and U.S. merchants to accept the new chip cards, enforced by a shift in liability for certain fraudulent transactions. By 2015, most other nations had already adopted chip cards, as the Congressional Research Service summarized, "leaving the United States as the last major country to implement what is now the de facto global standard."[22]

34. PIN verification (instead of the more fraud-prone signature verification) was required in most developed countries that adopted the new chip cards before the United States; these efforts became known by the shorthand "chip-and-PIN" or "EMV chip-and-PIN." In the UK, for example, a public-private partnership (heavily supported by the UK government, Visa, and MasterCard) promoted PIN verification with the slogan "I ♥ PIN." By 2006, 99.8% of chip transactions in the UK were PIN-verified.[23] A working paper prepared by a Federal Reserve Bank of Atlanta payments specialist concluded: "EMV chip-and-PIN has been highly successful [in] reducing domestic fraud in the UK."[24] Visa itself credited mandatory PIN with the significant decline in UK fraud: "The decline in Lost/Stolen and NRI [Not Received as Issued] fraud in the United Kingdom . . . is considered by Visa to be substantially, if not entirely, attributable to mandatory PIN@POS."[25] By 2012, nearly 75% of cards and 90% of POS

---

[22] Patricia Moloney Figliola, Cong. Research Serv., R43925, *The EMV Chip Card Transition: Background, Status, and Issues for Congress*, at 1 (Nov. 27, 2015), *available at* https://www.fas.org/sgp/crs/misc/R43925.pdf

[23] Douglas King, *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, at 5 (Jan. 2012) available at https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/120111wp.pdf

[24] *Id.* at 6.

[25] Form A, Exclusionary Provisions and Associated Cartel Provisions: Application for Authorisation, Public Version, Submission to the Australian Competition and Consumer Commission in support of the Application for Authorisation, Visa Worldwide Pte Limited and Visa AP (Australia) Pty Ltd (collectively, Visa) and MasterCard Asia/Pacific Pte Ltd (MasterCard), at 6 (July 4, 2013), attached as Exhibit A.

terminals in Western Europe had adopted the EMV chip-and-PIN standard.[26] The Visa Europe website for a time promoted the superiority of PIN verification on chip cards—it listed "Benefits of chip" such as "Increases customer confidence" ("Chip cards are harder to counterfeit and PINs help prevent fraud involving lost and stolen cards, which makes for more secure payment"), "Faster payment" ("Chip technology, especially when combined with PIN, helps to speed up service, cut queues, and reduce lost sales") and "Fewer disputes" ("Chip, especially when used with PIN, helps reduce fraudulent and disputed payments, saving you time and money on the administration around such payments").[27]

35. Canada similarly moved to a chip-and-PIN standard. Visa Canada announced its commitment to chip-and-PIN in June 2003 and shifted liability for certain fraudulent transactions in March 2011.[28] As a Federal Reserve Bank of Atlanta payments specialist concluded: "[S]ince the rollout of chip-and-PIN [in Canada], the EMV chip-and-PIN standard has been effective at reducing the types of fraud it is best suited to prevent—counterfeit and lost or stolen credit card fraud has decreased by 30 percent." [29] Visa Canada's website touted the "Benefits of Chip & PIN," saying chip and PIN brought "a new level of cardholder security and convenience." Visa Canada explained: "Chip cards and Chip terminals help make a secure transaction system even more secure by validating the cardholder's Chip & PIN. This enhances the security of your card whenever you use it in a face-to-face transaction." The combination of chip and PIN brings

[26] Douglas King, *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, at 7 (Jan. 2012) available at https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/120111wp.pdf

[27] Screenshot from www.visaeurope.com, attached as Exhibit B.

[28] Douglas King, *Chip-and-PIN: Success and Challenges in Reducing Fraud*, Retail Payments Risk Forum Working Paper, Federal Reserve Bank of Atlanta, at 13-14 (Jan. 2012) available at https://www.frbatlanta.org/-/media/Documents/rprf/rprf_pubs/120111wp.pdf

[29] *Id.* at 14.

"[i]ncreased security against unauthorized use [of] your card," Visa Canada explained: "Because your Personal Identification Number (PIN) replaces your signature, the transaction is more secure" (emphasis added). The chip and PIN combination also brings "[i]ncreased security against counterfeiting and skimming" because "[a] lost or stolen Chip card cannot be used to complete a transaction without its corresponding PIN. This technology virtually eliminates the ability to copy the contents of the chip to another card." Visa Canada argued that another benefit of PIN verification was "[g]reater convenience and ease of use" because "PIN entry replaces the need to sign a receipt."[30]

36. Australia has required PIN authentication (instead of signature) for most Australian chip card transactions (including debit card transactions) since August 1, 2014. Visa and MasterCard requested authorization from the Australian Competition and Consumer Commission to work jointly with each other and participating financial institutions to implement what Visa and MasterCard described as "mandatory PIN@POS in Australia" and to promote an education campaign called "PINwise." Visa and MasterCard's application touted the superiority of PIN verification over signature verification for fraud prevention: "Requiring the use of a Personal Identification Number rather than permitting signature as a means of customer authentication for all, or almost all, transactions at Point of Sale is a proven method of reducing card fraud."[31] Visa and MasterCard explained:

> [R]equiring the use of PIN removes the option of verification by signature; a less robust CVM. It is much more difficult for a fraud perpetrator to ascertain a PIN than to forge a signature. Accordingly, one of the most effective ways of

[30] Screenshot from www.visa.ca, attached as Exhibit C.

[31] Form A, Exclusionary Provisions and Associated Cartel Provisions: Application for Authorisation, Public Version, Submission to the Australian Competition and Consumer Commission in support of the Application for Authorisation, Visa Worldwide Pte Limited and Visa AP (Australia) Pty Ltd (collectively, Visa) and MasterCard Asia/Pacific Pte Ltd (MasterCard), at 1 (July 4, 2013), attached as Exhibit A.

> combatting fraud . . . is to make the use of PIN for customer verification compulsory.[32]

Visa and MasterCard urged the Australian Competition and Consumer Commission to act promptly, warning: "Any delay will prolong the period in which fraud perpetrators can take advantage of signature as opposed to PIN as a means of verifying a card at POS . . . ."[33] The Commission approved the application, with one publication reporting the result as "Visa and MasterCard join forces to ban the signature."[34] MasterCard applauded the Commission's approval; country manager Andrew Cartwright stated: "Use of a PIN saves time at the terminal, it's also a wise choice to help safeguard against fraud due to lost or stolen cards, as the chance of someone correctly guessing your PIN, which can be from four to six digits long, is very small."[35] Visa promoted the new protocol with a video saying "Meet Chip & PIN," "Here to Protect your Visa Card" "So You Can Enjoy Even Better Security": the voiceover said: "The new Visa Chip & PIN card gives you increased protection against fraud so you can shop, fuel, and do so much more with confidence."[36]

37. Most U.S. banks are following the lead of other nations in preferring PIN verification to signature verification with the new chip debit cards. The new chip cards allow the bank issuing the debit card to define, in order of priority, which cardholder verification methods (CVMs) are preferred in a transaction, and according to a June, 2014 report, from the Aite

---

[32] *Id.* at 6.

[33] *Id.* at 18.

[34] Kerry Lotzof, *Visa and MasterCard join forces to ban the signature* (Oct. 16, 2013) https://mozo.com.au/credit-cards/articles/visa-and-mastercard-join-forces-to-ban-the-signature/356068997

[35] Aimee Chanthadavong, *PIN@POS to become mandatory: ACCC gives green light to Visa, MasterCard* (Oct. 14, 2013) http://www.retailbiz.com.au/2013/10/14/article/PINPOS-to-become-mandatory-ACCC-gives-green-light-to-Visa-Mastercard/YAXLBOUTFK

[36] Available at: https://www.youtube.com/watch?v=Qb6amNuHTk0

Group, a research and consulting firm (made available to non-Aite Group subscribers by Visa): "[N]early all issuers interviewed plan to use chip and PIN as the preferred debit CVM."[37]

38. The banks' preference for more-secure PIN verification over less-secure signature verification is consistent with the reaction of U.S. consumers and others involved with the payment card system. For example:

- A March 2015 survey commissioned by MasterCard showed widespread U.S. consumer comfort with PIN verification with chip cards. The survey reported "Consumers view chip and PIN as most secure," and found: "Using a PIN to verify their chip card transactions continues to be the preferred way to use a payment card among all segments."[38]

- In May and June 2015, Randstad Technologies surveyed IT decisionmakers (including C-level staff) in large-scale national businesses (businesses with 100 or more locations) to gauge their reaction to the EMV transition. They reported: "The majority (66 percent) believe Chip and Signature does not offer ample security and that PIN technologies should be required."[39]

- In June 2015, Governor Jerome H. Powell—a member of the Board of Governors of the Federal Reserve System—delivered a speech in which he discussed ways to "enhance payment security." Governor Powell specifically questioned the continued utility of signature authentication, stating: "The deployment of EMV chip cards represents an important step forward. But we should not stop there. For many years, traditional authentication methods like signatures and static passwords have been used to verify that an individual is authorized to initiate a payment. New approaches to authentication increasingly offer greater assurance and protection. Given the current technologies that we have at our disposal, we should assess the continued use of signatures as a means of authenticating card transactions."[40]

---

[37] Julie Conroy, *EMV: Lessons Learned and the U.S. Outlook*, at 23 (June, 2014), *available at* http://www.mapacific.com/files/4282012/uploaded/Aite%20Report%20-%20EMV%20Lessons%20Learned%20and%20the%20U.S.%20Outlook.pdf

[38] MasterCard, *Consumer Enthusiasm and Desire for Chip Cards Growing* at 8 (May 2015), *available at* http://www.icba.org/files/ICBASites/NSPDFs/ChipCardConsumerAttitudes0515MC.pdf

[39] Randstad Technologies, *EMV Survey Results: Lack of time, deployment expertise cited as top obstacles to EMV readiness*, *available at* http://www.slideshare.net/RandstadUS/rt-emv-final

[40] Governor Jerome H. Powell, *Building a Safer Payment System* (June 25, 2015), *available at* https://www.federalreserve.gov/newsevents/speech/powell20150625a.htm

- In November 2015, eight state Attorneys General wrote a public letter to Visa and several financial institutions, urging them to "expedite the implementation of chip and PIN technology in the United States." The Attorneys General called signature verification a "less secure standard, since signatures can easily be forged or copied or even ignored at the point-of-sale." By contrast, the Attorneys General wrote, "[i]f employed here in the United States, PIN-based verification is likely to reduce fraud as is [sic] it has done in other places." The Attorneys General stated: "The chip and PIN approach is considered by many to be the gold standard currently for payment card security."[41]

B. Walmart's "Chip and PIN" Debit Card Protocol REDACTED

1. Walmart and "Chip and PIN" for Debit Cards

39. Walmart is the largest retailer in the United States, with total net sales (including net sales from Sam's Club, a membership-only warehouse club) of over $350 billion for fiscal year 2016, more than 5,000 retail locations employing 1.4 million people, and an online retail presence at www.walmart.com, www.samsclub.com, and www.vudu.com.

40. Debit cards are the most frequently used plastic tender in Walmart stores, accounting for over 70% of the dollar value of U.S. Walmart card payments. Walmart has accepted PIN debit and prompted cardholders to enter a PIN with debit transactions since the early 1990s. Consistent with Walmart's every-day low-pricing philosophy and its commitment to providing its customers with low-cost goods and services, Walmart does everything it can to ensure that its costs of accepting payment cards are as low as possible. Walmart also takes steps to ensure that the payment forms it encourages are safe and cost-effective. And thus, Walmart has long advocated for PIN verification (as opposed to signature verification) for debit transactions for many reasons, including PIN's demonstrated superior security and its lower cost.

41. Walmart publicly called for the United States to implement the "chip-and-PIN" standard used in other advanced nations. In 2010, Jamie Henry, Walmart's director of payment

[41] George Jepsen et al., Letter to Walter M. Macnee, et al. (Nov. 16, 2015), *available at* http://www.ct.gov/ag/lib/ag/press_releases/2015/20151116_chipandpinmultistateletter.pdf

services, said: "It's time for Chip-and-PIN in the U.S. Let's get a roadmap and move it forward here in the United States."[42] When Walmart upgraded its POS terminals to accept the new chip EMV cards, years before the 2015 deadline, it spent millions to make sure that the terminals had the ability to accept PIN verification because Walmart wanted to make sure that consumers would have the security of PIN verification and Walmart would have the ability to route debit card transactions over PIN debit networks.

42. In early 2015, Mike Cook, Walmart's assistant treasurer and a senior vice president, reaffirmed Walmart's preference for chip-and-PIN. "Signature is worthless as a form of authentication," Cook said. In reference to debit cards with PIN as the only form of cardholder verification, Cook stated: "If you look at the Target and Home Depot breaches . . . not a single PIN debit card needed to be reissued in those breaches," Cook said. "The card number was worthless to the individual thief and fraudsters, because they didn't know the PIN."[43]

43. In 2015, several banks and credit unions—including the Philadelphia Federal Credit Union, Provident State Bank in Maryland, AVB Bank in Oklahoma, and the Heritage South Community Credit Union in Tennessee—announced they would require PIN authentication for debit card transactions at Walmart. As Provident State Bank stated: "Effective immediately, you must provide your PIN number for all debit card transactions at any Walmart or Super Walmart."

44. In November 2015, Walmart instituted a chip-and-PIN protocol at some U.S. stores. Cardholders with chip debit cards were required to insert their card into a POS terminal

---

[42] Esther Schindler and Evan Schuman, *Wal-Mart: "It's Time for Chip-And-PIN In the U.S"*, FierceRetailIT (May 20, 2010), *available at* http://www.fiercecretail.com/story/wal-mart-its-time-for-chip-and-pin-in-the-u-s

[43] Jose Pagliery, *Wal-Mart exec: Credit card upgrade a 'joke'*, CNN Money (Apr. 3, 2015), *available at* http://money.cnn.com/2015/04/03/technology/walmart-credit-card/.

that could read the chip—the cardholders could not swipe their chip card at the POS magnetic stripe reader. Then, after cardholders inserted their chip debit card so the POS terminal could read the chip, they were required to enter a PIN code for verification—they could not bypass the PIN requirement by signing a receipt or signing electronically at the POS terminal. If a cardholder refused either to insert his or her chip debit card or to enter a PIN, then the transaction was declined and the cardholders was asked to use another form of payment.

45. This chip-and-PIN protocol was in the best interests of all concerned, particularly Walmart's customers: for one thing, it enabled Walmart, the issuing banks, and the cardholders to get the benefit of the chip technology by requiring the use of the chip instead of the magnetic stripe; for another, it enforced more secure customer verification by requiring customers to enter a PIN instead of permitting a signature. Walmart did not permit customers who claimed they did not remember their PIN to sign a POS terminal or receipt instead; such a workaround would have rendered worthless the enhanced security provided by PIN authentication. The chip-and-PIN protocol also saved Walmart money by permitting Walmart to route transactions over less-expensive PIN debit networks rather than more-expensive signature debit networks.

46. Walmart expanded the use of the chip-and-PIN protocol in January and February, 2016, rolling it out to approximately 3,700 U.S. stores by early February, 2016.

REDACTED

REDACTED

49. The Durbin Amendment directs the Board to prohibit network or issuer practices that "inhibit" merchant routing:

> [A]n issuer or payment card network shall not, directly or through any agent, processor, or licensed member of the network, by contract, requirement, condition, penalty, or otherwise, inhibit the ability of any person who accepts debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions.

15 U.S.C. §1693o–2(b)(1)(B) (emphasis added). Regulation II implements this direction:

> An issuer or payment card network shall not, directly or through any agent, processor, or licensed member of the network, by contract, requirement, condition, penalty, or otherwise, inhibit the ability of any person that accepts or honors debit cards for payments to direct the routing of electronic debit transactions for processing over any payment card network that may process such transactions.

12 C.F.R. § 235.7(b) (emphasis added).

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

REDACTED

V. CLAIMS

Count One—Declaratory Judgment

REDACTED

65. Walmart adopts and realleges all of the preceding paragraphs as though they were fully stated herein.

REDACTED

REDACTED

DEMAND FOR JURY TRIAL

Walmart demands a jury trial.

PRAYER FOR RELIEF

WHEREFORE, Walmart prays for relief and judgment as follows:

REDACTED

C. An award of the costs of the suit, including reasonable attorneys' fees; and

D. Such other and further relief as this Court deems just, equitable, and proper.

DATED this 10th day of May, 2016.

Neal S. Manne

NEAL MANNE (*pro hac vice* forthcoming)
nmanne@susmangodfrey.com
SUSMAN GODFREY L.L.P.
1000 Louisiana, Suite 5100
Houston, Texas 77002-5096
Telephone: (713) 651-9366
Facsimile: (713) 654-6666

DREW D. HANSEN (*pro hac vice* forthcoming)
dhansen@susmangodfrey.com

SUSMAN GODFREY L.L.P.
1201 Third Avenue, Suite 3800
Seattle, Washington 98101-3880
Telephone: (206) 516-3880
Facsimile: (206) 516-3883

ARUN SUBRAMANIAN
STEPHEN SHACKELFORD
CORY BULAND
SUSMAN GODFREY L.L.P.
560 Lexington Avenue, 15th Floor
New York, NY 10022-6828
Telephone: (212) 336-8330
Facsimile: (212) 336-8340
asubramanian@susmangodfrey.com
sshackelford@susmangodfrey.com
cbuland@susmangodfrey.com

JEFFREY SHINDER
JShinder@constantinecannon.com
CONSTANTINE CANNON LLP
335 Madison Ave., 9th Floor
New York, New York 10017
Telephone: (212) 350-2709
Facsimile: (212) 350-2701

DOUGLAS S. KANTOR (*pro hac vice* forthcoming)
KATE L. JENSEN (*pro hac vice* forthcoming)
STEPTOE & JOHNSON LLP
1330 Connecticut Ave., N.W.
Washington, D.C. 20036
Telephone: (202) 429-3000
Facsimile: (202) 429-3902
dkantor@steptoe.com
kjensen@steptoe.com

MICHAEL DOCKTERMAN (*pro hac vice* forthcoming)
mdockterman@steptoe.com
STEPTOE & JOHNSON LLP
115 South LaSalle Street
Suite 3100
Chicago, ILL 60603
Telephone: (312) 577-1300
Facsimile: (312) 577-1370

Attorneys for Plaintiffs