Defending Debit: A Historical Study of the Indirect Effects of the Durbin Amendment on Investment in Debit Card Security

Allison Miller
Electronic Arts
Workshop on the Economics of Information Security
June 2014

ABSTRACT

Regulations, even those not focused on information security, can have significant impact on security design, investment, or implementation for a system – depending on how that system adjusts to the externalities and indirect effects caused by the regulation. For policy makers and researchers, these ancillary effects can be difficult to predict since many factors – economic, political, social, and technological may be in play. This paper provides historical analysis of the indirect effects on debit card risk management (security, fraud prevention) of the Durbin Amendment to the Dodd-Frank financial reform act, including information that has become public in the wake of the recent Target Corporation data breach. Specifically, the paper shows how the Durbin Amendments' effect on the debit issuer business model has resulted in debit issuers having higher sensitivity to the costs associated with fraud/security, both the direct costs of fraud losses and the costs associated with investment in risk (security, fraud prevention) infrastructure.

1. INTRODUCTION

In the U.S. payments industry, while investment in risk management and security infrastructure has been a matter of interest for public policy (regulators, consumers), implementation of controls has been guided more directly by the commercial interests of participants (banks, merchants), with activities coordinated across the system by the payment card networks. Card networks have had the role of determining appropriate levels of investment and designing incentives that exchange pricing (fees paid, or revenues received) for liability for fraud issues or lack of compliance. Manipulating incentives has been an effective mechanism for upgrading fraud prevention capabilities historically, but in recent years the payment card networks have had mixed success encouraging step-level improvements in the risk management and security capabilities; perhaps due to low transactional fraud rates – or perhaps due to the need to evolve from controls that shift liability for fraud on a transactional basis into the more systemic controls needed to protect underlying infrastructure, and the indirect fraud exposure insecurity creates[1].

In the aftermath of a series of data breaches, the card networks have been criticized for their perceived inability to accelerate adoption of more secure underlying infrastructure, such as data tokenization, the EMV chip standard (sometimes described as "Chip-and-PIN" or "Chip-and-Signature") technology in the acceptance environment, or point-to-point encryption processes – suggesting that the payment industry as a whole has underinvested in security infrastructure. Other commentators point out system fraud

[1] Varian, Hal. "Managing Online Security Risks." *New York Times*; New York, N.Y.; Jun 1,2000.

rates are still near historic lows, argue other technology may more appropriate to invest in, or are requesting that legislators step-in to determine if liability allocations are fair and reasonable for all participants in the system. While we do not take a position on investment strategy or liability schema in this paper, we do propose that further efforts (regulatory, commercial interests) to encourage security investment in the payments industry, or introduce security regulations for the participants in the payments industry, need to factor-in incentives created by non-security related regulations. Our primary finding is that non-security related externalities may dominate incentives designed to encourage security-related investments.

To understand the impact of non-security related regulations we selected the Durbin Amendment, a portion of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, which is primarily concerned with controlling price on the card network interchange fees charged to merchants for debit card transactions, and routing options. The Durbin Amendment does not specify requirements for issuer or merchant risk mitigation practices such as criteria for protecting card data, security infrastructure, privacy requirements, nor does it change liability for fraudulent transactions or consumer protections from unauthorized access/charges on their accounts. We evaluate whether introduction of this externality for debit card issuers affects their approach to risk mitigation or investment in security infrastructure, by reviewing pre-Durbin practices/investments, and comparing them with post-Durbin practices, that are either new for the debit card issuers or newly differentiated from the practices of credit card issuers (or debit card issuers that are excluded from the Durbin amendment).

Related works assess topics such as technology adoption and innovation in the payments infrastructure[2], information security/breach policies in U.S. retail payments[3], dynamics affecting fraud trends/prevention[4], and cybercrime measurement[5]. There are fewer works examining externalities unrelated to security/privacy/fraud and then assessing the impact of those externalities to security investments and related strategies. Therefore as background we provide additional context of the payment industry dynamics (specifically business model and revenue drivers, relevant to a regulatory externality concerned with pricing) and available risk mitigation options, so that effects of Durbin, as a new factor, are more easily discernable when evaluating a differences in response patterns to a security event (card data breach), and in infrastructure investments more generally.

These findings will be useful to regulators who are considering introducing legislation or incentives on payment card industry participants, and will also be useful to researchers who want to create more realistic models of how the payment card industry will respond to potential changes (regulations, introduction of new security technologies). Based on this research we also see opportunities to further examine the related roles of liability shifts (intra-system or imposed by external regulators) and pricing

---

[2] Anderson, Ross. "Risk and Privacy Implications of Consumer Payment Innovation." PDF available at http://www.cl.cam.ac.uk/~rja14/Papers/anderson-frb-kansas-mar27.pdf

[3] MacCarthy, Mark. "Information Security Policy in the U.S. Retail Payments Industry." Workshop on the Economics of Information Security, June 2010.

[4] Sullivan, Richard J. "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy." For presentation at the 2010 Workshop of Economics of Information Security. May 21, 2010.

[5] Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the cost of cybercrime". (2012) PDF available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf.

to understand the impact of incentive design on changing investment behavior and resolving coordination issues, especially as relates to security infrastructure in network markets[6].

There are many challenges that face analysts/researchers looking at payment card industry risk. The system is complex, with many participants seeking to optimize their performance based on different incentive structures and business models. It is difficult to measure the impact of changes made to the system (introducing a technology, incentive or cost) since much of the activity in the system is unobservable to outside analysts. Likewise risk mitigation investment and operational strategies of individual participants are not generally publicly available.

Given the goal of the paper and the challenges for analysis, the plan for the paper is as follows. Section 2 provides relevant background on the debit card business model, and its development/growth prior to the introduction of the Durbin Amendment. This section is meant to provide some background for readers who may not be familiar with the payment card industry or differences in debit issuance versus credit issuance. We will also review risk mitigation strategies, specifically breach-response practices for card issuers, in a "pre-Durbin" context. (Breach response is a component of overall risk mitigation strategy that may affect infrastructure investment, and that yields some discernable information about risk tolerance in the short-term). Section 3 provides an overview of the Durbin Amendment; its purpose as well as the direct effects on debit issuers since its introduction. In Section 4 we examine breach response and related risk mitigation strategies/investments post-Durbin, primarily as characterized by issuer response to the Target breach. In Section 5 we will review our Findings based on comparing pre-Durbin to post-Durbin investment options and breach response practices. Finally, Section 6 presents a discussion of findings, and recommendations to policy-makers and researchers on key takeaways and recommendations for incorporating our findings into their research.

2. Card Issuance (Pre-Durbin)

For most of their history, payment card networks in the U.S. were primarily associated with credit cards (or charge cards, in the case of American Express), until the late 90's when branded "signature" based debit cards began to be widely available to consumers. Through the early 2000's the debit category continued to grow quickly, and in 2008, total dollar volume of purchases made using Visa Inc.'s branded debit cards surpassed credit-card purchases for the first time, with $206 billion in U.S. debit-card transactions processed making up 50.4% total transaction volume in the last quarter of 2008, up from about 40% in 2003[7].

The card networks connect two kinds of financial institutions.

- Acquiring banks have a contractual relationship with merchants, and are together discussed as the acceptance environment, since they accept payment cards for purchase. Merchants pay acquirers for the ability to accept cards (the "discount rate" which includes interchange;

[6] Background material on pricing in the context of framing security problems: Camp, L. Jean and Wolfram, Catherine D., "Pricing Security: Vulnerabilities as Externalities." Economics of Information Security, Vol. 12, 2004. Available at SSRN: http://ssrn.com/abstract=894966

[7] Sidel, Robin. "Debit-Card Use Overtakes Credit." Wall Street Journal Online. Updated May 1, 2009. http://online.wsj.com/news/articles/SB124104752340070801

interchange is set by the payment networks and the discount rate by acquiring banks).

- Issuing banks have a contractual relationship with account-holders (who may be consumers, small businesses, or even commercial institutions). Merchants/acquirers pay the issuers an amount for each transaction, which is called "interchange". Depending on the issuer's relationship with the account-holder, they may also receive revenues (such as annual fees or interest on a line of credit) from their account-holders directly.

For credit card issuers, the transactional revenues received from merchants in the form of interchange fees are generally a smaller portion of revenue than the interest and fees the banks receive from their credit cardholders. Debit card issuers, on the other hand, do not receive interest payments from account-holders as debit cards provide access to deposit products. Revenue from fees – interchange fees received from merchants, and service fees (like overdraft) on deposit accounts drive the checking account business model – and debit cards are typically provided as a feature of a checking account. The Durbin amendment that we will discuss is regulation specifically designed for debit card issuers.

Overview of Debit Business Model

The development of debit cards with national payment brand acceptance at point-of-sale with signature (and in some cases PIN) authentication were a useful business model innovation for consumer banks, as access to DDA's (demand deposit accounts) was previously a cost center, not a revenue center, to maintain. Before the card networks introduced these "branded" debit cards, consumers typically accessed DDA funds via personal checks or institutional means (EFT, wire transfers). With the introduction of ATM technologies, retail banks were able to offer customers a more efficient (and low-risk, since cardholders authenticated via a PIN instead of the risky and easily forged personal checks) mechanism to access their funds[8]. ATM networks were, in the 90's, primarily a run via agreements between regional debit networks[9]. There was competition between the PIN networks and transactional pricing was relatively low. Both PIN- and signature-based debit volumes grew rapidly during this time period, mostly displacing checks as a portion of consumer payment volume. Visa and MasterCard both created their own networks (Plus and Cirrus, respectively), which were managed separately from the networks' credit card processing systems.

Regarding ATM-based debit product acceptance at the point-of-sale (POS): while there were some ATM networks that were able to make the move from ATM machines to POS systems at retail locations, card-based payments at the point of sale were still dominated by the large card networks like Visa and MasterCard, that worked with banks to issue credit cards. Leveraging their position on retail POS systems, the card networks facilitated the implementation of a new kind of debit card that, like ATM cards provided consumers with access to a DDA account, while gave merchants the ability to leverage their existing signature-based acceptance systems. For the issuing banks, these signature-based debit cards commanded the higher-margin transactional revenues associated with interchange fees, generally higher than the fees charged in a PIN-based ATM transaction. Interchange fees can vary widely – even in

---

[8] Quinn page 23. https://www.frbatlanta.org/filelegacydocs/er08no4_QuinnRoberds.pdf

[9] Interbank networks of the 90's, like MAC or Tyme, were regional and did not overlap, but had inter-network agreements for acceptance across larger geographies. i.e. cards issued by one network would be honored almost anywhere ATM/POS cards were accepted for payment. More details on debit networks can be found here: *http://en.wikipedia.org/wiki/Debit_card#United_States*.

the U.S. – based on factors such as merchant processing volume, data presented during the authorization request (full magnetic-stripe versus key-entered), and card product being used by the consumer (business versus consumer account)[10]. For example, in 2013 the average credit card interchange for a Visa premium, card present transaction was about 2.1% per transaction[11], while a similar PIN-based transaction earned the issuers about $0.30 per transaction or a fee of approximately 0.69% of the average transaction volume[12].

When assessing the revenues associated with card issuance, it is also useful to keep in mind that while credit and debit cards have similar functionality, the business model associated with credit issuance is quite different from that of debit. Credit card issuers earn, in addition to interchange, the interest charged to cardholders on credit line balances. In February 2014 the average annual percentage rate (or APR), for variable-rate credit cards was around 15% while the APR for fixed-rate cards was around 13% (where was for most of 2013)[13]. Debit cards, most commonly provided by banks as a product bundle with checking accounts, are not associated with lines of credit. In fact they are considered to be more like a feature of a checking account product, and the debit card revenues (from interchange fees) are considered part of the retail bank's checking account revenues (including overdraft and monthly service fees) and DDA profitability. Thus, while interchange is a small component of credit card product revenues, which is driven by the interest earned from the associated lines of credit, debit card interchange is the only revenue source for the debit cards, which are evaluated as one component of the deposit product business model.

Retail banks responded to the better revenues associated with signature-based debit transactions by encouraging their DDA customers to use signature-based debit rather than ATM cards as a way to access their funds both from ATM/cash dispensers (still PIN-based) and at retail locations accepting Visa and MasterCard (signature-based). At the same time, banks begin offering additional services to deposit holding customers. It is as debit penetration was rising that U.S. customers[14] began to see:

- Free checking, with lower or no minimum balances
- Free ATM transactions
- Reward programs for signature based debit at retail locations

Essentially, adding the incremental revenue from debit interchange allowed the banks to provide low-cost or free checking and rewards features to customers. It seems like a safe assumption that some of these additional features, which benefited consumers and small businesses, were being subsidized by the fees paid by card accepting merchants. Debit card overdraft fees also provided additional revenue to

---

[10] MasterCard 2013–2014 U.S. Region Interchange Rates: PDF available here: *http://www.mastercard.com/us/merchant/pdf/MasterCard_Interchange_Rates_and_Criteria.pdf*

[11] Federal Reserve Bank of Kansas City, Payments System Research Department, "Credit and Debit Card Interchange Fees in Various Countries, August 2013 Update." PDF available at: http://www.kansascityfed.org/publicat/psr/dataset/Intl_IF_August2013.pdf

[12] Board of Governors of the Federal Reserve System. "Average Debit Card Interchange Fee by Payment Card Network." Last update: August 2, 2013. http://www.federalreserve.gov/paymentsystems/regii-average-interchange-fee.htm .

[13] Herron, Janna. "National credit card rates for Feb. 27, 2014." *Bankrate.com* http://www.bankrate.com/finance/credit-cards/rate-roundup.aspx.

[14] Primarily these services were offered to consumers, but banks also tailored offers to small businesses.

retail banks' checking products. (Supporters of Durbin seem focused on the issue that pricing may have been set unfairly based on the alleged Visa/MasterCard duopoly dictating acceptance practices at retail POS locations more than they seem concerned about how the revenue from interchange is used at issuing banks.)

PRE-DURBIN RISK MITIGATION: OPTIONS FOR ISSUERS RESPONDING TO CARD BREACHES

Issuers, whether they are issuers of debit or credit products, have risk mitigation strategies designed to manage their exposure to transactional fraud losses. Typically strategies include compliance with industry best practices related to card manufacturing, distribution, and issuance, adoption of available authentication/fraud reduction services available through the card networks, and also investment decisions by the issuers related to authorization and authentication technologies and practices. The methods for managing transactional fraud losses apply whether the fraud (counterfeit, stolen, improperly authorized) occurs on a single card or on a group of cards across a portfolio. However with the increase in large-scale card breaches that have occurred in the past few years, significant portions of an issuer's portfolio may be exposed to heightened risk very suddenly, creating a need to issuers develop plans and practices for addressing these compromised cards in response to the breach, as opposed to "normal" fraud screening practices.

When a breach of card data comes to light, however it is discovered, issuers have a few choices about what they can do to protect themselves and their customers from the potential fraud that can occur from compromised cards that are still active and "open to buy". The first step is that the breached entity will share with the card networks any card data that is suspected to be compromised, and it will get loaded into a system that associates compromised customer data back to the issuing bank[15]. Next issuers will be notified (receive an alert) if there is data waiting for them in the system. Visa's version of this storage and notification system is called CAMS[16], and issuers access the CAMS system to obtain information about breach events and the cards in their portfolio that may have been compromised due to the security breach

Once an issuer has received a set of potentially compromised accounts, they have two processes to kick-off. One is related to customer notification; compliance obligations vary by geography but customers will require notification if any of their personally identifiable information has been compromised. The second process is a defensive process: the steps they will take to prevent subsequent fraud that could take place on compromised cards.

Let's break the options into two categories; reactive strategies and proactive strategies.

REACTIVE STRATEGIES

Reactive strategies will include the options an issuer has for reducing fraud associated with a single breach event; these are short-term steps requiring resources be applied immediately and then a short-tail as far as for how long the defensive strategy is going to be effective at stemming fraud losses from compromised cards. Reactive strategies include reissuance of compromised cards, and steps to restrict

---

[15] Card numbers are split up by BIN (Bank identification number), i.e. the first six digits of the 16-digit PAN. Each BIN is associated with an issuer, issuers may operate multiple BINs. Note this requires the cards be available in plain text to the card network to complete the segmentation.

[16] http://usa.visa.com/download/merchants/what-every-merchant-should-know-GCAR-VOL-091213-final.pdf

authorization strategies.

Reissuance

Reissuance is the simplest step an issuer may take to addressing incoming fraud from a data breach; canceling the compromised card means that there will be no potential for fraud coming in from that payment instrument. The upside is this is very effective for reducing exposure to downstream fraud. The downside is that it can be expensive (banks estimated in late 2013 that card reissuance was costing on average $10 per card[17]), it can be a poor customer experience, and that "suspected compromised" does not necessarily mean a card will ever be used fraudulently; in fact in 2013 banks estimated 1 in 3 compromised accounts had subsequent fraud take place[18]. Though banks may be required to notify any account-holder that has been potentially compromised, banks are able to choose their own re-issuance strategy, and as such can opt to reissue:

- **Full** – Full reissue is when the issuer cancels and reissues all cards associated with a breach event. In a large compromise event, issuers may lack the systems capacity to simultaneously reissue all compromised cards and may have to reissue groups of cards in "waves."
- **Risk-based** – Risk-based is when the issuer evaluates their account-holder portfolio, and either a) identifies higher- and lower-risk segments of the portfolio so that some segments are reissued their cards and others are not, or b) segments the portfolio in order to stage the reissuance over a long period of time[19].

Restricting Authorization Strategies

For issuers that do not conduct a full reissue, taking steps to restrict their fraud screening is typically used to reduce chances that risky transactions from compromised cards result in fraudulent charges. Restrictions can be simple and harsh, or more sophisticated and risk-based:

- **Simple Caps –** Criteria for declining a transaction can also be very simple, such as "$200USD per day limit on ATM withdrawals" or "decline all card-not-present transactions". These simple caps are effective at reducing exposure to fraud transactions, but harsh, as many legitimate cardholder transaction attempts will be declined as well as potential fraud transactions. With debit cards, the "harshness" includes an issuer's arbitrary restriction of customers' access to funds on deposit ("their money"). Within authorization strategies there are already implied limits on behavior, for example "number of transactions that will be allowed within 24 hours". Depending on the options available within the authorization system[20], these types of limiting

---

[17] Kitten, Tracy. "Card Breaches Pose Greatest Fraud Risk." *InfoRisk Today Podcast*. February 7, 2014. http://www.inforisktoday.com/interviews/card-breaches-pose-greatest-fraud-risk-i-2178

[18] Kitten, Tracy. "Target Breach: The Cost to Banks." *InfoRisk Today Podcast*. February 12, 2014. http://www.inforisktoday.com/interviews/target-breach-cost-to-banks-i-2182

[19] For example a bank might segment their customers by customer lifetime value, or by spending frequency. A bank might decide high-value customers should receive their replacement cards before the compromised card is canceled, so as to give them the best customer experience possible. A bank might decide that fraud transactions on a high-frequency spending card are going to be more difficult to detect/prevent, and prioritize frequent spenders for reissuance immediately, with customers who are inactive or infrequent spenders to be reissued at the end of the reissuance cycle.

[20] FICO's Falcon Fraud Manager is popular system for issuers choosing to outsource their decisioning platform, with a set of standard variables on which to build authorization strategies http://www.fico.com/en/products/fico-falcon-fraud-manager/.

variables will be used in combination, such that some set of "risky" behaviors occurring on the same transaction will then invoke a behavioral limit, after which transactions will either be flagged for review or outright declined.

- **Compromised card strategy** – A "compromised" strategy, or set of strategies, is a more sophisticated approach to limiting exposure of fraudulent transactions which allows compromised cards to be left open to buy, but incorporates additional monitoring and more restrictive fraud-screening on transactions attempted. Authorization strategies are typically segmented, major segments might separate customers by "type" (consumer versus business), by account age, geography, or other groupings that allow for most optimized fraud screening.
    - Compromised strategies typically mimic an existing set of strategies, but might lower per-day limits, restrict use of cards to the account holder's local geography, and alert more frequently at unattended terminals (like automated fuel dispensers at gas stations) that may be associated with card testing activity. Compromised strategies may also restrict access to cash or quasi-cash at point of sale locations or card-present environments that sell high-value, easily resold merchandise that is attractive to fraudsters. For example, limitations on medium to high dollar transactions at grocery stores, pharmacies and post offices (which sell prepaid cards and money orders), and also high-ticket transactions at office supply stores, big box retailers, and jewelry stores (computers, consumer electronics, and jewelry can be easily fenced or resold)[21].
    - Another accommodating strategy might be to determine high- or low-risk by authorization channel. For example an issuer might look at a debit portfolio and see there is a segment of customers who primarily use their cards at ATM machines. If PINs have not been compromised, those customers' subsequent ATM transactions are low risk, and an effective authorization strategy could be to restrict use of their cards at retail point-of-sale locations, but leave the cards set to authorize at ATMs[22].

There are some considerations (pre-dating the introduction of Durbin) that might cause debit issuers to manage their risk controls differently than credit issuers, or have incentives to engage in different levels of investment in security infrastructure. For example:

- **Sophistication of authorization strategies:** Credit card issuers have more experience making complex decisions at time of authorization, as they have been managing both credit and fraud risk on lines of credit, with a signature-based authorization system for years[23]. Debit issuers, however, developed out of a PIN-based acceptance environment: until the emergence of signature-debit products, the debit issuer primary "question" to answer at time of authorization was whether or not the account-holder had balance sufficient to cover the transaction for which

[21] Issuers can code strategies specific to the MCC (Merchant Category Code) of an acceptance location, but are unable to incorporate specific items purchased into their risk decision. Technically purchase of money orders or prepaid cards would be correctly specified as "quasi-cash", equivalent to a cash advance, but this coding is a default setting on the terminal/point-of-sale system and so is typically set to the merchant's category rather than adjusted per transaction.

[22] Acceptance channel category (ATM, PIN-based point-of-sale, Signature-based point-of-sale, CNP (Card Not Present) are data elements available in the authorization request for issuers to evaluate, and tune their strategies accordingly.

[23] As a category credit card issuers have more (years of) experience in designing/managing authorization strategies, but this statement is not meant to imply that a given debit card issuer is necessarily less sophisticated in their implementation of authorization strategies than a credit card issuer.

authorization was being requested. The weaker level of authentication provided by signature-based acceptance required debit issuers to upgrade their authorization capabilities in response to the different acceptance technology to keep fraud losses in-check[24]. Another factor that may influence sophistication of authorization strategies for credit issuers versus debit issuers: credit and debit card portfolios are often managed out of different areas in a bank (since credit cards are associated with lending, and debit cards associated with balance-holding DDA/checking accounts), institutions may have separate technical as well as analytical implementations of their authorization capabilities.

- **Fast feedback loop:** Anecdotal data from issuers suggest that debit card holders are more likely to notice and quickly report unauthorized charges against their DDA/checking account than credit card holders[25], with the rationale that consumers feel a stronger sense of ownership and concern about the funds in their checking account (their money) versus charges on a line of credit (the bank's money).
- **Customer impact:** Though U.S. consumers have zero liability for unauthorized charges on their Visa and MasterCard accounts, reducing a checking account balance – even temporarily - is considered a worse customer experience than reducing the "open to buy" on a line of credit. It is a major inconvenience for account holders to not have access to their money, even if eventually they get the funds back, resulting in higher customer service costs. Also, for many years when debit accounts were accessible through cards primarily via PIN-based transactions, dispute resolution was not as clear-cut, as the stronger authentication meant it was more difficult to differentiate false claims from true victims in the dispute resolution process – taking longer to restore stolen funds, and frustrating legitimate account holders suspected of submitting inaccurate claims.

Despite these differences in breach response consideration between debit and credit card issuers, prior to Durbin there was negligible differences between card issuers response reactive strategy selections based on debit vs credit card type.

PROACTIVE STRATEGIES

Proactive strategies will include the options an issuer pursues for reducing exposure to fraud risk in the longer term, these may require significant resources be applied for years before generating a payoff as far as reduced exposure to fraud, but there is a long-tail expected for stemming fraud losses from compromised cards. Proactive strategies include investment in advanced authorization systems, acceptance-side prevention, or adaption of business model.

Advanced Authorization Systems

Authorization systems are the systems that approve or decline transactions being attempted by the customer, at the point of acceptance. An authorization strategy is a set of rules or logical conditions that make the approval or decline decision. Incorrect approval and decline decisions have costs associated

[24] As an alternative to pursuing more sophisticated authorization strategies, debit card issuers could choose to invest in additional authentication technologies, including "Chip-and-PIN" at the point of sale. Pre-Durbin, there is not much difference between credit and debit issuer adoption/investment in such technology.

[25] Discussion at 2014 eFraud forum, RSA, reviewing call center trends and contact rates, especially as leading indicators of card data compromises, and the differences in sensitivity to unauthorized activity of debit versus credit cardholders.

with them: incorrect approvals can admit unwanted fraud to the system, and incorrect declines represent an opportunity cost (lost revenue) and also may have customer service impacts/costs[26]. Selecting an authorization strategy requires the issuing bank clarify how they want to handle the trade-off between incoming fraud (catch rate) and incorrect declines (false positive rate). An issuer's selection of the point of trade-off reflects their sensitivity to the different risks posed by incorrect decisions. Let's say for now that risk averse issuers will have a bias towards fraud/cost reduction (focus on catch rate) and risk seeking issuers will have a bias towards revenue expansion (focus on hit rate i.e. reduction of false positives).

From the combination of fraud controls/data and technology available to transaction authorization systems, a set of strategies can be built and the best strategies will be implemented, let's call this an entity's risk horizon – the expected performance of their best performing strategy. It is useful to clarify that some entities may, finding their current authorization trade-offs unacceptable, wish to make step-level improvements to authorization strategies as a whole. This can be done by investment in technology (faster systems, smarter systems, or better data), that allows for the emergence of higher performing authorization strategies[27].

Acceptance-Side Prevention

An alternative to improving fraud detection within authorization systems is to improve the security technology at the point of sale, to make it more difficult to present fraudulent cards successfully for a point-of-sale transaction, or to make it more difficult to make counterfeit cards in the first place. The most popular acceptance-side solution is Chip-and-PIN, the EMV version that has been widely adopted in Western Europe. EMV is the de-facto standard and implementation in the U.S. has begun, albeit slowly: "…in the U.S., 4.5% of card-present transactions originate from chip terminals, primarily at big box merchant locations like Walmart and Best Buy... [and as of early 2012]…Visa announced that U.S. financial institutions have reported issuing an estimated one million Visa-branded, EMV chip-enabled cards as of the end of 2011. It should be noted that there are well over a billion Visa-branded credit cards in the U.S., so this one million EMV chip-enabled number is a very small percentage.[28]"

However, while experience in Europe has shown using dynamic authentication at the point of sale (instead of the static authentication data on the magnetic stripe) has had a positive impact on fraud rates on domestic transactions, fraud rates in fallback scenarios and in card-not-present channels

---

[26] Some background: performance of an authorization strategy is typically evaluated on two key dimensions: catch rate and hit rate. Catch rate is an inclusion metric; how many of the bad transactions attempted are prevented by the authorization strategy. So, a random strategy might, out of 1000 transactions, if the strategy declined 10% of the transactions, it should randomly have caught 10% of the fraud attempted. Hit rate is an accuracy metric: of the transactions identified as fraudulent, how many of them were actually fraudulent? For example if 100 transactions are flagged as fraud transactions, and 85 of them were actually fraud, that is an 85% hit rate. (Conversely, 15% of the transactions were incorrectly identified as fraudulent, so the strategy would have a 15% false positive rate – hit rate = 1-false positive rate).

[27] Theoretically, a shock to the system or removal of data/available technology may force the issuer to an inferior curve, but under normal circumstances an rational entity would not abandon a well performing authorization strategy in favor of a poorly performing authorization strategy.

[28] TSYS whitepaper. "U.S. EMV Adoption: Lessons Learned from a Canadian-Based Value Added Resource (VAR)." 2012. http://www.tsys.com/acquiring/engage/white-papers/United-States-EMV-Adoption.cfm#5

continue to be a challenge[29]. Given that Western Europe has the highest adoption rates of EMV cards (80.7%) and of EMV terminals (94.5%) in the world it is not surprising that fallback scenarios continue to be an issue (for comparison, Asia Pacific has card adoption rate of 26.7% and EMV terminal adoption rate of 50.5%).

Further, since launch EMV has been criticized for vulnerabilities in both design and implementation of the system, with flaws described including insider attacks (at banks), PIN verification attacks (on the terminal), pre-play attacks (exploiting improper random number generation), and transactional misreporting by the terminal[30]. In addition to the fact that existence of these flaws means that widescale adoption may be followed by a new wave of exploits, these vulnerabilities are especially pernicious because root cause of the fraud transaction is obscured, which is a critical issue, as payment system dispute resolution processes rely on understanding what kind of fraud has occurred and where[31].

While imperfect, most experts agree that the technology underlying EMV chip is superior to magnetic stripe when it comes to reducing counterfeit. However, given the cost of moving the system to new acceptance technology, some industry experts have suggested that looking at newer alternatives and "leapfrogging" chip-based solutions altogether. In her article on EMV, Webster points out that in 2013 the payments networks floated the concept of creating a cloud-based tokenization standard, and that the combination of mobile and cloud-based technologies could be as secure (if not more secure) than EMV chip. Webster also believes the newer technology solutions might ultimately provide superior customer experience, as the EMV chip system requires more cardholder involvement in the point of sale process (including remembering PINs, which can be a barrier to completing the sales process in some situations)[32].

In any case, investment in the acceptance infrastructure requires coordination of many participants in the payment card industry, and given the expense associated with upgrading the system, many issuers choose to focus their proactive investment dollars into systems wholly under their control, namely their authorization systems, or direct-to-account-holder authentication options. The card networks have endorsed EMV chip system for U.S. acceptance infrastructure upgrades, and as an attempt to resolve the coordination issue, created a liability shift that will go in to effect for most of the network participants in late 2015. Network participants passing transactions using the EMV chip system (for card issuers this means EMV chip cards and associated authorization decisions, for card merchants this means EMV chip-enabled acceptance devices) will be protected from liability for fraud should transactions later be disputed as fraudulent.

---

[29] An instructive example related to fallback scenarios: "The UK demonstrated significant drops in fraud rates for lost/stolen cards after complete implementation of EMV. BUT, and it's a big BUT, fraud losses for phone, Internet and mail order skyrocketed, dwarfing the prior losses in lost/stolen. In the U.S., fraud occurring over digital and phone channels represents 40 percent of the losses but only 5 percent of the sales." (Colgan)

[30] Murdoch 2

[31] Murdoch 3

[32] Colgan

The liability shift date and timeline are factors that issuers and merchants can factor into investment decisions going forward. Before the liability shift was announced, adoption of the EMV chip technology would be based on the investor's understanding of the efficacy of the technology as well as the likelihood that EMV chip implementation would achieve a relevant critical mass among other participants. It makes sense that uncertainty around the adoption timeline encouraged issuers to adopt a "wait and see" approach, since in the card present space where EMV chip is relevant, card issuers already have primary liability for the counterfeit problem that EMV chip addresses. Having a firm liability shift timeline reduces some of the uncertainty around return on investment.

Prior to Durbin, proactive strategy preferences/selection appear to be largely independent of portfolio card type (debit vs credit) in the sense that very few issuers of either type have begun issuance of EMV chip cards. However, a cursory review of EMV chip enabled cards available from U.S. issuing banks today suggests that the cards are marketed primarily to international travelers and premium account-holders, i.e. credit card products, or other card products with high margin business models[33].

3. The Durbin Amendment

The Durbin Amendment refers to an amendment to the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 that set price controls on interchange fees that debit card issuers may charge to merchants accepting said cards, and also prohibit issuers and networks from controlling/limiting how debit card transactions may be routed[34]. The amendment also makes provisions for merchants to allow surcharging or set minimum transaction amount for card processed transactions – previously these practices had been prohibited by Visa and MasterCard operating rules. Passed by Congress, the law took effect in October 2011. In March, 2014, the Court of Appeals for the D.C. Circuit overturned a lower court ruling by D.C. District Judge Richard Leon, ruling that the Federal Reserve Board did not exceed the authority granted to it by Congress in promulgating rules regarding the cap on debit card interchange fees and routing requirements pursuant to the Durbin Amendment (part of the 2010 Dodd-Frank Act)[35].

The amendment is focused on the interchange fees charged by large banks (small banks and credit unions are excluded from the price caps). Some subcategories of debit, like prepaid/payroll/gift cards are excluded from the price caps[36].

Opinions on Durbin

Supporters of the Durbin amendment believe the interchange model creates undue costs for small businesses and consumers, since small businesses pay higher interchange (due to their lower volume), which represents a disproportionate component of their potential profits. These acceptance costs may be passed on to consumers in the form of higher prices. In addition, the additional fees generated by

---

[33] For example https://www.creditcardinsider.com/learn/chip-and-signature-chip-and-pin-emv-cards/

[34] Board of Governors of the Federal Reserve System. "12 CFR Part 235, Regulation II; Docket No. R-1404: Debit Card Interchange Fees and Routing. Final Rule." PDF available at: http://www.federalreserve.gov/aboutthefed/boardmeetings/20110629_REG_II_FR_NOTICE.FINAL_DRAFT.06_22_2011.pdf

[35] http://www.coxsmithbanking.com/d-c-court-of-appeals-overturns-judge-leons-lower-court-ruling-on-durbin-regulations/#.U2745cbzjvw

[36] Cardhub

interchange may be suppressing competition among debit networks as the high fees commanded by Visa and MasterCard create an incentive for issuers and the card networks to exert their influence across the payments ecosystem to see that transactions are routed away from the lower cost debit networks and towards Visa and MasterCard systems (or the systems that command higher fees).

Also, as Levitin points out, deposit accounts are a "gateway relationship" that allow a bank to cross-promote other, more profitable, products (like loans, investment services, or insurance)[37]. Hence a secondary impact of Durbin, beyond the price caps meant to lower fees merchants pay into the card system, is to give smaller banks (theoretically excluded from the price caps) and advantage in the market[38].

Detractors of Durbin point out that the cost of accepting debit payments – even at credit card interchange pricing – is still on average a lower cost burden than handling cash, checks and ACH transactions, and that the products and features enabled by debit interchange (free checking, free ATM transactions, rewards program) are unlikely to be matched by merchants in lower prices in retail establishments, and that the pricing caps set by the regulators are unlikely to cover the true cost of managing risk (securing, preventing fraud) on debit card transactions[39]. Also detractors point out that the exclusions provided to prepaid cards are likely to encourage banks to simply switch out their debit programs for reloadable gift cards, and that the exclusions for small banks/credit unions are unlikely to work in implementation due to the complexity and lack of transparency in how payment transaction routing occurs[40].

Another criticism of Durbin is that the entities that appear most likely to benefit from the price caps are large "big box" merchants like Target and Wal-Mart, who have the scale to negotiate low interchange and the sophistication to introduce their own prioritized routing for payments accepted in their retail locations – and that the further reduced pricing will improve their profitability, but cost savings may not be shared with consumers in the form of lower retail prices.

INITIAL IMPACT

The proponents and critics of the Durbin Amendment are still arguing about whether or not the legislation is successful, should be further amended, or fully repealed. However:

- Large U.S. debit issuers' interchange revenue is cut roughly in half, but they are paying lower network fees than small banks (4 cents lower for signature, 2 cents lower for PIN)[41]

---

[37] Levitin 1

[38] Unfortunately one of the problems with implementing Durbin (and one of the reasons small banks and credit unions have also been looking for Durbin to be further amended or repealed) is that some of the routing-related requirements in the bill mean that, based on how transactions are routed, small banks may also end up receiving capped (lower) interchange revenue.

[39] MasterCard published a statement labeled "Interchange and the Durbin Amendment" (undated, but accessed in February 2014, http://www.mastercard.com/us/company/en/docs/Interchange_and_Durbin.pdf) had this to say on the topic of cost recovery: "The Fed's ultimate decision…sets interchange fees at levels that will, under the Fed's own analysis, prevent issuers from recovering the vast majority of the costs associated with offering debit card products and services."

[40] Sekhar 3

[41] Levitin

- Small banks' interchange rates are higher than large debit issuers (50bps more as a rate, or 31 cents advantage on signature and 8 cents advantage on PIN)
- Small banks' market share of debit card transactions grew slightly[42]
- Large debit issuers have slashed rewards programs, and are slowly introducing fees on checking products
- Challenges to the debit regulation have yet to resolve whether the caps adequately cover fraud costs borne by issuers, or whether merchants may need to support additional costs for fraud reduction[43]
- Timelines for EMV (the expected chip-card acceptance technology that will replace current magnetic stripe devices/acceptance technology) migration have not been adjusted, but industry participants recognize that the rulings may have an affect EMV adoption in the U.S.[44]

Given that the Durbin amendment is still relatively new, full impact on debit issuers, merchants, processors, and consumers is not yet clear. But early indications show that the Durbin amendment has a direct financial impact on the business model of debit issuers (reduced revenues and profit margins), and reduces costs of accepting debit card transactions to merchants.

4. Post-Durbin Risk Mitigation: Target Breach as a Case Study

Security and fraud prevention in the payments infrastructure has been a hot topic in recent years, due to a series of high profile data breaches (and the subsequent fraud losses), including Cardsystems International (40M records, 2005), TJ Maxx (94M records, 2007), and Heartland (130M, 2009)[45]. It is clear the payment card infrastructure has become a popular target for attacks – in 2013 payment card details were the most popular target for identity data thieves, beating out social security numbers (the primary target in 2012). And the downstream effects for consumers of being included in a breach were worse: 46 percent of consumers who had their debit cards breached in 2013 become fraud victims within the same calendar year, compared to only 16 percent of consumers who had a Social Security number breached[46]. Breach activity has been high enough that card manufacturers/distributors have credited the trend with the higher demand they're seeing for plastics[47], a trend also noted by journalist Brian Krebs who reported that some issuers with plans to reissue cards were delayed by order backlogs

---

[42] Levitin

[43] Morrison

[44] EMV Migration Forum. Executive Director of the EMV Migration Forum Randy Vanderhoof remarked: "While the court's decision to overturn the current interchange ruling affects transaction economics, the court's ruling regarding debit transaction routing requirements has the bigger impact on planning for EMV migration. It calls into question whether at least two debit routing choices are required for each card, or for each transaction. This can impact the technical implementation of EMV for debit and its multiple industry stakeholders."

[45] Sullivan 6

[46] Kitten, Tracy. "Card Breaches Pose Greatest Fraud Risk." *InfoRisk Today Podcast.* February 7, 2014. http://www.inforisktoday.com/interviews/card-breaches-pose-greatest-fraud-risk-i-2178

[47] During Fidelity National Information System's (FIS's) 2013 fourth-quarter earnings call", Gary Norcross, president and chief operating officer at FIS, noted that, while the processor doesn't do much on the acquiring side, the company has seen increased demand for cards because of the recent breaches." (Green)

at the card manufacturers[48].

These trends aside, the Target breach is the first major breach to occur in the wake of the Durbin Amendment and thus instructive for understanding if debit issuers have adjusted their security practices in response to their changed business model. 40 M cards were compromised in Target breach.[49] Expenses linked to the data breach at Target Corp. have already cost the 58 member institutions of the Consumer Bankers Association more than $170 million, with more than 17.2 million debit and credit cards reissued as of February 2014.[50]

From the perspective of this analysis, the Target breach is an interesting case to examine due to 1) how it was discovered (not through information security checks or compliance audits at the compromised entity/merchant but from the fraud prevention systems of issuer banks) and 2) the difference between how credit and debit card issuers responded (best characterized by Chase, who not only initiated spending caps on their customers but publicized their strategy (extremely unusual)).

How the breach was discovered: One might assume a breach would be identified by auditors, operational staff, or because the "hack" is publicized by the attackers themselves. But in this case, the breach was identified by downstream system participants. Specifically card issuers, whose fraud detection systems were able to see anomalous activity and isolate the security breach back to Target[51]. We mention the detection method as it shows the deep connection between infrastructure security and fraud prevention technology, as, in the payments infrastructure, they are complementary risk management investments.

Issuer reaction to breach: Post-breach, the press and industry commentators remarked upon the potential high impact on card issuers with statements such as: "[Issuers perceived the Target breach to be severe and creating high exposure, and] ...consequently banks were forced to impose blanket account restrictions and limits as a knee-jerk reaction to prevent significant losses because they didn't have real-time visibility into what was happening with individual accounts.[52]" However this is not accurate. All issuers (both debit and credit issuers) received similar notifications of compromise activity, and had real-time visibility into the transactions (including risky transactions) via their existing authorization systems. A more accurate statement would be that, several debit issuers instituted harsh spending caps and limits (typified by Chase, who publicly their revised authorization strategies for debit after the

---

[48] Krebs, Brian. "Card Backlog Extends Pain from Target Breach." Krebs on Security. February 14, 2014. http://krebsonsecurity.com/2014/02/card-backlog-extends-pain-from-target-breach/

[49] Krebs, Brian. "Cards Stolen in Target Breach Flood Underground Markets." Krebs on Security. December 20, 2013. http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/

[50] Kitten, Tracy. "Target Breach: The Cost to Banks." *InfoRisk Today Podcast.* February 12, 2014. http://www.inforisktoday.com/interviews/target-breach-cost-to-banks-i-2182

[51] The industry term for this practice is "Common Point of Purchase", and it requires correlation of cardholder payment activity and corresponding potential fraud transactions; what is striking about the Target example is in the past identifying CPP happened in the center of the system (at a system operator like Visa or MasterCard), but in this case a major issuer had enough cardholder volume - and sophisticated enough systems - that both the anomalous behavior and the source were correctly identified.

[52] Skeen

Target breach[53]), and this particular strategy in responding to the breach appears to be a unique to debit card issuers.

In addition to the caps and limits introduced by debit card issuers, there is another difference in the response to the Target breach that is significant: that the changes to the Chase authorization strategy were publicized. Typically, other than reissuance strategies, issuers do not share changes they make to their authorization practices in the wake of a breach.

Other issuer post-breach response: Another element to consider is what we did not see from debit issuers, which are expedited plans to migrate to more secure infrastructure such as EMV chip or (for card-not-present transactions) 3D Secure. In the wake of the breaches of holiday season 2013, both Chase and Bank of America announced expedited release of chip cards – on their credit products. EMV chip will benefit from a transactional fraud liability shift in 2015, and 3D Secure benefits from an existing liability shift, however are not being pursued aggressively by debit card issuers.

So far since the Durbin Amendment went into place[54], we've seen debit issuers respond to a large security breach using reactive approaches that appear to be aimed at cost reduction in the short-term, as opposed to proactive investments to reduce exposure in the long-term. Further, we see some debit issuers deviating from previous practices that they used to share with credit card issuers, specifically they appear to be abandoning the use of finely tuned authorization strategies and selective reissuance in favor of restrictive activity/spending caps and wide spread reissuance[55].

Our hypothesis is that the Durbin Amendment's direct effect on debit issuer business models (lowering interchange) has had the indirect effect of creating a higher sensitivity to potential fraud losses – as issuers have a lower margin in which they can tolerate incoming fraud transactions. To wit:

- When a transaction occurs, the issuer earns interchange (for example, 2%).
- When a transaction is fraudulent, the issuer must reimburse the customer for the face value of a transaction, minus the fees received for processing the transaction[56] (98%).
- For one fraudulent $100 transaction, the issuer will need to successfully process 49 equivalent $100 transactions to break-even (from a fraud perspective, other costs excluded from this example).
- With interchange roughly halved, (for example to 1%, the same issuer would need to

---

[53] Note: All other factors being equal, size of an issuer's portfolio will have a large impact on the effectiveness of their authorization strategy, simply because there are more data points to correlate, and enough scale to develop useful segments. Banks with smaller portfolios (regional banks, credit unions) have sparser data on which to train their authorization strategies. However the issuer that went on the record for introducing harsh caps as a response to exposure to compromise was not a small bank, but Chase -- one of the world's largest banks and payment processors, a bank known for proactively identifying fraud trends in their payment processing activity (i.e. an issuer with sophisticated authorization technology), and Chase chose to ONLY introduce the harsh caps on potentially compromised cards in their Debit portfolio.

[54] Liability shifts, reporting requirements, technical controls in place at issuers and in the Acceptance environment, and other administrative details of security breach management remain the same.

[55] Henry, David. "Millions of Target shoppers face new debit card limits." Reuters.com, Dec 21, 2013. http://www.reuters.com/article/2013/12/21/us-target-jpmorgan-idUSBRE9BK0D020131221

[56] In general, if the issuer has a chargeback right on a card transaction, they process a chargeback for the transaction amount and interchange. If the issuer does not have a chargeback right, they will keep the earned interchange.

successfully process double the number (i.e. 98) $100 transactions to make up for one fraudulent transaction.

The post-Durbin debit card revenue model also introduces the concept of flat pricing, i.e. $0.25 per transaction, whether the transaction is $2 or $2,000. This means that insomuch as each transaction is "risky" at some level:

- A debit card issuer has a higher risk exposure, in absolute terms and relative to the potential revenue, on a $2000.00 ($0.25 upside, $2000 downside) transaction than a $2.00 transaction ($0.25 upside, $2 downside).
- To keep costs of fraud losses stable (in absolute dollars of fraud), current state of fraud prevention practices will suffice
- To keep impact of fraud losses (as a cost component relative to the revenue earned), debit card issuers would have incentives to tune authorization strategies to be more sensitive to risky high-dollar transactions, or to curtail risk exposure above a certain transaction dollar amount by stricter limits.

This is an interesting point, that the Durbin debit card revenue model means in every transaction the issuer receives roughly the same compensation, but that transactions do not have the same risk exposure. The penny of transaction fees allocated by the Federal Reserve meant to cover fraud costs may be ample if the average transaction amount is $5 (a penny would cover up to a 20bp fraud rate, roughly 4x current system fraud rates) the allocations may not suffice is the average transaction amount is $50 (a penny would cover a 2bp fraud rate, which is less than 1/3 the current system fraud rate). It is likely that fixing fraud tolerances in this manner will influence issuer authorization strategies to be more conservative as they are motivated to manage expected losses into acceptable bounds, given their business model.

Post-Durbin, debit issuers appear to be more reactive than proactive in their approach to risk mitigation (as evidenced by response to card data breaches), adopting simple, loss-avoidant strategies, even at the expense of good transactional activity that might occur above rigid spending caps. What is less clear is what will happen in the medium to long term. In the current incentive structure, debit issuers may double-down on their reactive approach and delay implementation of improved technology such as EMV chip in order to avoid the expense of an upgrade – even though long-term cost of fraud losses plus prevention strategies may be higher. Moving to delay implementation of EMV chip could be seen as a strategic move if the debit issuers believe implementation of chip technology will be slow despite the liability shifts going into place next year, or if they believe that the card networks may lose resolve and delay or cancel the liability shift. Delayed implementation of EMV chip may also occur in situations where the appropriate funding for managing a debit card portfolio is unavailable (due reduced revenues, or some other business model issue).

It remains counter-intuitive that an issuer's increased sensitivity to losses is paired with less willingness to invest in proactive risk-reduction. However as a set of investment decisions, the behavior can be explained if the strategy is simply to reduce all costs associated with debit card portfolio management. Along with cutting services (such as rewards programs to cardholders) could come cost-cutting opportunities associated by "cutting" any relaxed authorization strategies made available to customers seeking to access their deposits using a signature-authenticated transaction at the point-of-sale. Foregoing revenue to keep costs low is not an investment strategy associated with a growing product

category; if this sensitivity to costs is widespread among debit issuers in the medium- to long-term it provides additional insight into the impact of Durbin on the debit issuer business model and supporting infrastructure investments that can be expected.

5. FINDINGS

In summary, while the Durbin Amendment did not include any direct obligations for changing debit security technology, risk management practices, or fraud prevention techniques, the changes to the debit issuer economic model have had a significant impact on how debit issuers manage and invest in security technology and risk controls in the short-term. The financial impact of fraudulent transactions is relatively larger for debit card issuers than credit card issuers, given reduced margins and parity authorization technology. The medium- to long-term impact on debit issuer investment strategies is more difficult to assess, as payment card infrastructure is prone to coordination challenges when making step-level system-wide improvements, and other participants show mixed commitment levels to upgrade underlying security infrastructure, for example from a magnetic stripe-based system to EMV chip-based technology (specifically chip-and-PIN).

Our method for analyzing the effect of the Durbin Amendment on debit issuer risk mitigation practices has been to:

- Review debit business model and card issuer security/risk practices before the Durbin Amendment, checking to evaluate differences between debit and credit issuer practices.
- Examine the direct effects of Durbin, and identify if there requirements specified to issuers related to security/fraud management technology or process.
- Assess issuer security/risk practices following Durbin, to determine if different approaches are being used, and further to clarify if any changes in practices are differentiated based on issuer portfolio type (credit vs debit).

We specify that:

- Pre-Durbin: In the U.S., credit and debit issuers had similar security, fraud prevention, and breach response practices.
    - However regarding EMV chip implementation, credit issuers appear to be more likely to have adopted chip than debit issuers.
- Durbin: The Durbin Amendment does not specify requirements to Issuers related to security, fraud prevention, or breach response.
    - However fees earned on debit interchange are both (on average) lower and also fixed, with a penny of the $0.22-0.25 in fees allocated to fraud prevention for qualifying issuers.
- Post-Durbin: We observed differences in debit issuer breach response, as debit issuers appeared more likely to impose spending limits/caps, and a large debit provider engaged in a new process as part of the breach response: publicizing their changed authorization strategy.
    - Also, some issuers have announced expedited plans to upgrade acceptance infrastructure to EMV chip, but in reference to their credit – not debit - cards

Based on the Target breach, we observe that credit issuers responded to the Target breach in a similar

manner to previous breaches, but that debit issuers varied – specifically by introducing more stringent, reactive strategies. Publicly communicating the spending limits provided the market with an additional signal that at least one debit card issuer's risk tolerance had been reduced to the point that 1) the issuer was willing to forego revenues on transactions above the spending limits and 2) it was necessary to adjust the expectations of consumers who sought to access their deposits both via PIN- and signature-based card transactions. Further, though a liability shift rewarding investments to security infrastructure and card issuance was published, reducing uncertainty in return on security investments, no debit card issuers sought to reduce their transactional fraud exposure through upgrades to EMV chip or the existing liability protection of 3D Secure. Therefore we conclude that the introduction of Durbin had an effect on debit card issuers' approach to risk mitigation and investment as a negative externality.

Our best explanation for this is that the Durbin direct effect on debit revenues (on average lower, and now fixed) has resulted in debit issuers having a lower tolerance to fraud losses in the short-term, and their reduced margins are resulting in a cost-avoidant outlook and lower willingness/ability to invest in risk (security, fraud prevention) infrastructure.

Available data supports the central thesis that non-security related externalities may dominate incentives designed to encourage security-related investments. However the conclusions reached in this paper should still be treated as preliminary for several reasons: 1) though it has been about six months since the news of the card data breaches occurring in holiday season 2013, most of the data available on impact was collected early in the breach response cycle, 2) adoption of acceptance technology like EMV chip (and 3D Secure) in the U.S. is still limited and so differences between debit and credit adoption of these card products cannot yet be discerned, and 3) at the time issuers were responding to the holiday season card breaches and the initial research for the paper was conducted, there was an open challenge to the Durbin Amendment waiting for a decision that would have been impactful to the pricing controls described in this paper, and that further, debit issuers may have been waiting for a final decision on the challenge before committing to longer-term risk-mitigation decisions like infrastructure investment. Now that the challenge has been decided (pricing controls set by Durbin were upheld), it will be useful to see if there are similar patterns in breach response (such as higher sensitivity of debit issuers to fraud loss exposure) as observed during the Target breach. We also will have to wait and see if differences in EMV adoption continue to existing between debit and credit issuers; data on acceptance infrastructure investment will be easier to measure though it will take longer to collect. Access to better performance data on issuance criteria, authorization strategies, authentication adoption, and breach detection practices would also be useful for validating our hypothesis or confirming our understanding of investment decisions and drivers[57].

[57] Performance data that would be useful to compare between debit and credit issuers (that is not generally available but would provide support for modeling debit versus credit risk mitigation strategies) include daily/monthly spending limits, average transaction size, average number of fraud transactions occurring on a compromised card before detection, PIN- versus signature-based transaction volumes, distribution of fraudulent transactions for a portfolio across merchant category codes, etc.

6. Discussion

In 2000, Hal Varian (in a response to Ross Anderson's paper "Why Cryptosystems Fail[58]") made an observation on the economics of payment system security that is still provides useful context in 2014: that liability in payment systems can be an effective incentive for banks to make the right investments in risk management (if constructed carefully), and that in general, the state of "computer security is so poor in practice because liability is so diffuse"[59].

When security fails in the payment infrastructure, the most obvious impact is the fraud losses that result from stolen payment data or "hacked" acceptance infrastructure. And while losses from fraud have been rising steadily for the past 20 years, loss rates are still near system lows. In 2012 global losses from fraud (including issuers, merchants, and acquirers of credit, debit, prepaid and private label payment cards) reached $11.27 billion, up 14.6% over previous years. However gross fraud loss rates (which increased from 5.07bp in 2011 to 5.22bp in 2012) remain near historic lows. And while PIN-based transaction have fraud rates at the lower end of the spectrum (1.1bp) compared to the global card brands (Visa, MasterCard, Amex, etc.) at 6.13bp, in the U.S., issuers remain primarily responsible for most of the losses (64% of $5.33B USD) – mainly at point of sale from counterfeit cards – while merchants/acquirer losses (36% or $1.92B USD) occurred primarily on card-not-present transactions[60].

The participants in the system still do not seem to agree on whether security problems are correctly invested against, much less whether liability is allocated effectively. However there is limited transparency from which outsiders can evaluate the extent of issues caused by payment system insecurity: better information sharing between participants (currently only issuers are notified of breach events) could help clarify whether investment levels are appropriate or under-allocated.

Policy-makers concerned about high dollar value of fraud losses may want to consider that the low loss rates may be part of the reason that investment in security infrastructure has not been a top priority for participants in the payments industry, given the costs associated with making step-level improvements. If participants were unable to absorb fraud losses into their profit margins, there would be more interest in wide-scale adoption of more secure infrastructure and practices. Even absent transactional liability, the system-wide impacts of insecurity may be enough to encourage participants to begin solving their coordination problems using more proactive methods and investments. Public/private partnerships to assess the technical options and examine potential impact of different implementation strategies could be especially useful in this area.

When it comes to security infrastructure and risk controls, coordination problems are typical in the payments industry. What the payment card networks have done in the past to encourage (or mandate) adoption of new technologies introduced is to, in a targeted way, manipulate incentives. The two levers used are pricing and liability for fraud, both affecting transactional cost. CVV, AVS, CSC/CVV2, and 3DSecure were all implemented in this way using manipulations of transactional pricing or fraud liability (See Appendix A for a timeline). It is unclear, however, whether or not such an approach will

---

[58] Anderson, Ross. "Why Cryptosystems Fail" Prepared for ACM Conference on Computer and Communications Security, 1993. http://www.cl.cam.ac.uk/~rja14/Papers/wcf.html

[59] Varian

[60] The Nilson Report (news release via Business Wire)

work with EMV chip; while simple pricing incentives and liability shifts have sped adoption of many features and successfully gained traction for many transactional fraud controls, the liability shift put into place for 3DSecure was NOT effective in the US (though many U.S. issuers support 3DSecure, adoption in the U.S. is still limited).

Additional research into economic incentives that would be compelling for different participants in the payment system (merchants, processors, issuers, card systems) could yield options (such as vulnerability "pricing" strategies[61]) that augment the current payment system methods of transactional incentives (pricing or fraud liability), and compliance programs, without upsetting the intra-system transaction processing schema. Since payment industry security is by nature systemic and not transactional, developing a set of tools or requirements that exist outside of the payment network schema may be necessary to align the interests of participants effectively.

Finally, we recommend policymakers and researchers consider engaging participants in the payment system that have not been discussed in detail: the account-holders themselves. Since U.S. consumers have limited liability for fraudulent transactions[62] (or "zero-liability" for Visa and MasterCard), they are largely seen as participants who are not interested or not willing in making investments in infrastructure security. But with 46 percent of consumers who had their debit cards breached in 2013 becoming fraud victims within the same calendar year[63], consumers may be more willing to engage, if only to prevent inconvenience associated with card replacement and sorting out the details of unauthorized charges on their accounts. Business account holders have even greater incentives to participate in "self-defense" of their accounts, as they do not enjoy the protection of Reg E & Reg Z, and may be liable for unauthorized access to their accounts. Encouraging "opt in" programs that provide improved or out-of-band authentication at the point-of-sale might be a viable step-up mechanism for system security.

Coordination problems in network markets like payment processing can be difficult to solve absent the ability to design strong direct incentives, and sensitivity of participants to the direct and indirect effects of externalities. While insecurity in the payments infrastructure continues create issues for system participants, as yet the system has not been able to agree on the right level or method of investment, and we recommend policy makers and researchers conduct additional examination of applicable incentive design and investment options, to ensure participants are adequately protected and consumers' interests are defended, no matter what kind of payment method they are using.

---

[61] Camp, L. Jean and Wolfram, Catherine D., "Pricing Security: Vulnerabilities as Externalities." *Economics of Information Security*, Vol. 12, 2004. Available at SSRN: http://ssrn.com/abstract=894966

[62] This has not always been the case, and consumer liability limitations are due to legal requirements, as opposed to driven by the card networks.

[63] Kitten, Tracy. "Card Breaches Pose Greatest Fraud Risk." *InfoRisk Today Podcast.* February 7, 2014. http://www.inforisktoday.com/interviews/card-breaches-pose-greatest-fraud-risk-i-2178

APPENDIX A: EVOLUTION OF RISK CONTROLS IN THE PAYMENT CARD INDUSTRY

Evolution of technology risk management and fraud prevention in the payments infrastructure, a few key milestones are described below. These controls described are the controls/services required by the payment industry – for the most part these controls/services were designed and adopted based on internal drivers (i.e. card network rules and requirements) as opposed to being required by external regulators.

This timeline also shows how the card networks have facilitated fraud prevention improvements, as typically the controls require buy-in from both the issuing side (card issuing banks) and the acceptance side (merchants). In some cases support also is required from intermediate processors (i.e. flags and message formats must be supported from end-to-end of the system. To resolve coordination issues across the network, the payment network has routinely attempted to design appropriate economic incentives (typically in the form of liability shifts) to encourage appropriate participation.

The control itself (security measure, control, practice, or service) will be designed, then economic incentives will be constructed that encourage one set of entities to participate (merchants to act, issuers to provide a service). The incentives that work best (are implemented most quickly) are direct, meaning they provide a liability shift for associated fraud transactions or affect pricing (costs borne or revenue received). When one set of entities has reached a critical mass adoption, the incentive is typically adjusted to encourage the rest of the system participants to also buy-in.

For example the upcoming liability shift for Chip-and-PIN will first shift liability for counterfeit-related fraud transactions at the point of sale AWAY from issuers and on to the merchants that do NOT adopt the recommended infrastructure/practices. Today issuers are responsible for counterfeit fraud losses so this is a negative incentive for laggards.

EARLY 1990'S –ANTI-COUNTERFEIT THROUGH BETTER AUTHORIZATION PRACTICES

Dumpster-diving carbons: Counterfeit plastics

- Problem: Fraudsters were able to create counterfeit cards good enough to pass a merchant's physical inspection and with enough information to obtain an authorization from the issuer from discarded carbons used in the manual
- Solution: A cryptographic value (the CVV, "card verification value) was included on the magnetic stripe. When full magnetic-stripe data was passed to the issuer (during an online authorization request), the issuer could validate that it was a valid card. Including CVV as a component determining liability for fraud (1992). In addition merchants were encouraged to request online authorization and provide full magnetic-stripe to the issuers via pricing incentives and chargeback protection (Custom Payment Service, 1993).

Skimmers: Counterfeit cards

- Problem: Fraudsters were able to gain full magnetic stripe value from cards that they were able to "swipe" either by surreptitiously double-swiping a card at a retail point-of-sale, or by deploying skimming devices in unattended card acceptance devices (e.g. ATM machines, automated fuel dispensers at gas stations).
- Solution: A limited solution, but the card brands have over the years made several attempts to create visual cues for card acceptors and law enforcement to differentiate "real" cards from the

copied version. For example, screen-printing as well as engraving parts of the 16-digit PAN, placement of the branded holograph on engraved area of the card, microtype on the signature panel. Implementation of this control primarily occurs at card manufacturers, who provide cards meeting the card network standards to issuing banks (ongoing).

MID-1990'S -2000: ISSUER-PROVIDED CONTROLS FOR CARD-NOT-PRESENT

Stolen card information: Verifying address

- Problem: Mail Order and Telephone Order (MOTO) merchants (for example, catalog businesses) found themselves unable to provide full magnetic stripe data (anti-counterfeit) or to obtain a cardholder signature at the point of sale (the available method for validating the cardholder). As such the card not present environment created a loophole for fraudsters in possession of card data that could be stolen or "phished[64]" from victim cardholders.
- Solution: The card networks conceived of a service (implemented in the U.S., U.K., and Canada) by which issuers would confirm the "billing" address provided by a cardholder was valid (i.e. matched the billing address on file)[65]. Support for AVS became mandatory for issuers, as a component of fraud liability, circa 1995.

Stolen card information: Validating Card in Possession

- Problem: Address verification was not enough to prevent losses at MOTO and e-Commerce merchants, as knowledge of a cardholder's billing address was easily reconstructed from non-card-related data associated with identity theft victims, phishing scams, and customer database compromises. The card networks tried to come up with a complement to the CVV that would help participants in the transactions feel more confident that the payer attempting to checkout did in fact have the card in their possession at the time of checkout.
- Solution: A second cryptographic value was generated and printed on the signature panel of the card, so that it could be easily used by a cardholder on the phone or online with the merchant, but that the merchant would use only to gain a positive validation from the issuer, and would not need for customer service purposes. In fact the merchants were expressly prohibited from storing the CVV2 (also known as the CVC2, CSC, or CID) so that the code would retain value as an anti-fraud mechanism, even in the face of transmission or loss of card-related data[66]. CVV2 went global as a component of fraud liability in 1998.

---

[64] In this context "phishing" will serve to describe any method of tricking a cardholder out of their details, whether via a "phishing" email, fake web storefront, fraudulent inbound telemarketing, or other social engineering attempt.

[65] The Address Verification Service works off of the leading numeric and postal code provided by the cardholder, and there are multiple response types. The requirement of the issuers is to respond in good faith; their obligation is to provide the matching service, while the merchant can interpret the response given their own risk appetite. For example, an issuer may respond back with an AVS "no match" and a positive authorization and fulfill their obligation. The liability shift occurs only when the issuer fails to provide a response upon request for AVS.

[66] Like the Address Verification Service, the issuer's responsibility is to provide a response code (match/no match variants) if validation of the CVV2 is requested. Once the code is provided, the merchant's subsequent interpretation of the code (whether to proceed or decline the sale) is a risk back upon the merchant.

Stolen card information: Validating Cardholder is Present

- Problem: While CNP merchants were liable for fraud, they had limited information to work from to differentiate good customers from potential fraudsters. The entities that were in the best position to make an effective authorization decision were still the issuing banks, who could identify patterns indicating fraud across their account holder's spending activity across multiple merchants, but who were no longer liable for the transaction. Both merchants and issuers were lacking a mechanism for positive authentication of the account-holder at time of transaction.
- Solution: The card networks developed the 3D Secure protocol (branded by Visa as Verified by Visa and by MasterCard as MasterCard Secure Code), which allowed for an out-of-band authentication event to be connected to the authorization process. Account holders need to enroll in the service (to pick their PIN or password), and then within the checkout flow (for merchants that integrated the service) customers would be redirected to an authentication flow hosted by (or on behalf of) their issuer. Positive authentication would result in a code being shared with the merchant (called the CAVV), which was then included in the authorization request – and began being included as a component in fraud liability in 2003[67].

2000's: Plugging Fraud "leaks" From Acceptance Environment

Dumpster-diving receipts: PAN usage

- Problem: Fraudsters were able to use card information routinely printed on customer receipts to conduct identity theft, create counterfeit cards that could be used under floor limits or at merchants with limited acceptance technology/practices, or to conduct transactions at card-not-present locations.
- Solution: Card networks mandated that merchants remove critical card details from receipts; this required acceptance devices either remove details by default or be configurable. Truncating cardholder details was required by federal law (Fair and Accurate Credit Transaction Act (FACTA); passed in 2003 merchants were given several years to phase in new acceptance technology and comply[68].

Card Data Breaches: Cross-network payment system security issues

- Problem: Card data at merchant locations, but outside traditional point-of-sale systems (i.e. in customer databases, as opposed to just the card swipe systems) began being targeted at card-not-present locations that tended to maintain historical transaction records. The insecurity of breached entities created fraud liability at issuers and downstream merchants/acquirers, so the card networks also wanted to adjust their liability guidelines to address these situations, so that redress for breaches could occur within the payment system without needing to involve third parties (like courts, or legislators).
- Solution: The card networks developed a "standard" or set of best practices, that were meant to guide participants to protect card data in storage and in transit. In the early 2000's, these compliance programs were run independently by the different card brands. To avoid repetition

---

[67] However implementation of liability shift has varied by region. http://www.fraudpractice.com/gl-vbv.html.

[68] http://www.business.ftc.gov/documents/alt007-slip-showing-federal-law-requires-all-businesses-truncate-credit-card-information-receipts

or misalignment, the card brands turned to the Payment Card Industry (PCI) forum to manage a common set of requirements and compliance program going forward. The PCI Security Standards Council launched in 2006, and is responsible for the development, management, education, and awareness of the PCI Security Standards, including the Data Security Standard (PCI DSS), Payment Application Data Security Standard (PA-DSS), and PIN Transaction Security (PTS) requirements.

Small-fraud adds-up: Sub-floor limit activity, UAT's

- Problem: Floor limits were designed to allow for risk-limited offline acceptance (i.e. without a real-time, online authorization response) at merchant locations. Floor limits were developed to allow for greater acceptance in areas where merchant locations had limited access to cheap telecommunications, for merchants engaged in low-ticket transactions that typically did not draw a lot of fraud, or for business models that were low-risk and better suited to batch processing of transactions (merging authorization and settlement/clearing processes) in daily files rather than incremental messages. In the U.S. telecommunications were available relatively cheaply (compared to some areas in Europe and also in developing markets), however there were high fraud losses associated with sub-floor limit transactions, which issuers had to accept despite the fact they'd not had an opportunity to make an authorization decision at the time of transaction (the issuer would be notified about the transaction at the point of settlement/clearing). Floor limits varied by merchant category code; a typical floor limit in the U.S. might have been something like $50 floor-limit on transactions at convenience stores, which would allow a counterfeit card (not previously reported lost or stolen) to be used for transactions under $50 without need for the merchant to obtain a positive authorization from the card issuer. Unattended terminals (UAT's, and also cardholder activated terminals, CAT's) requiring high through-put (classic case is UAT's at toll collection points) were a known loophole vis a vis floor limits.
- Solution: In the U.S. $0 floor limits were introduced in 2007, this obviated future fraud losses from sub-floor-limit transactions, as the removal of floor limits means that issuers will have the ability to make an authorization decision on all transactions.

Augmenting authentication in card-present: Chip and PIN (EMV)

- Problem: In Europe Chip-and-PIN was developed as an stronger option for offline authorization of cardholder transactions (as telecommunications costs were historically high). In the U.S., where telecommunications have been inexpensive, the card networks and issuers had less incentive to continue to support offline acceptance. However, in recent years, despite advanced analytics and authorization capabilities at the time of transaction, issuers still experience a great deal of fraud activity, driven by counterfeit cards. The EMV implementation of chip and PIN would provide stronger authentication at the point-of-sale via the dynamic (rather than static) verification process that occurs between the chip card and the terminal (authenticating the card is valid) and the PIN-entry of the cardholder (authenticating that it is the card owner participating in the transaction).
- Solution: A timeline for U.S. implementation of Chip-and-PIN implementation was announced in 2011, but implementation has been slow. Visa and MasterCard Card Associations released strategies, timelines, and incentives for US merchants, issuers, and acquirers to move from

magnetic strip authentication to the EMV standard by 2013[69]. More recent timelines show a liability shift is expected to go into place in 2015, though U.S. implementation of EMV is still not widespread.

[69] https://www.burlingtonbankcard.com/home/articles/emv-in-the-us-adoption-timelines-and-incentives-from-visa-and-mastercard/

REFERENCES

Anderson, Ross. "Risk and Privacy Implications of Consumer Payment Innovation." PDF available at http://www.cl.cam.ac.uk/~rja14/Papers/anderson-frb-kansas-mar27.pdf Paper presented at "Consumer Payment Innovation in the Connected Age" conference took place March 29-30, 2012, in Kansas City, Mo. Conference proceedings available here http://www.kc.frb.org/publications/research/pscp/pscp-2012.cfm.

Anderson, Ross, Chris Barton, Rainer Bohme, Richard Clayton, Michel J.G. van Eeten, Michael Levi, Tyler Moore, and Stefan Savage. "Measuring the cost of cybercrime". (2012) PDF available at: http://weis2012.econinfosec.org/papers/Anderson_WEIS2012.pdf. Camp, L. Jean and Wolfram, Catherine D., "Pricing Security: Vulnerabilities as Externalities." Economics of Information Security, Vol. 12, 2004. Available at SSRN: http://ssrn.com/abstract=894966.

CardHub. "Interchange Fee Study – Durbin Amendment." Cardhub.com, operated by Evolution Finance. Last updated 2012, available at http://www.cardhub.com/edu/interchange-fee-study-2010/.

Colgan, Gloria. "EMV: Solving For The Wrong Problem." Pymnts.com. 23 September 2013. Available at http://www.pymnts.com/briefing-room/issuers/trends-in-debit-cards/2013/the-durbin-amendment-briefing-room/EMV-Solving-For-The-Wrong-Problem/.

Contardi, James, David S. Evans, Bill Gajda, Tracey Kitzman, Robert Litan, Upendra Namburi, and Richard Schmalensee. "The Net Effects of the Proposed Durbin Fee Reductions on Consumers and Small Businesses." *Lydian Journal*. February 2011, pdf available at http://www.pymnts.com/assets/Lydian_Journal/LydianJournalMarchEcon.pdf.

EMV Migration Forum. "U.S. EMV Migration Efforts Continue Despite Debit Regulatory Challenges." *Globe Newswire*, October 3, 2013, available at http://globenewswire.com/news-release/2013/10/03/578027/10051162/en/U-S-EMV-Migration-Efforts-Continue-Despite-Debit-Regulatory-Challenges.html.

Green, Jeffrey. "EMV Now Seems Assured; Should U.S. Payments Firms Readjust And Stick To Their Roots?" Pymnts.com. 06 February 2014, available at http://www.pymnts.com/briefing-room/security-and-risk/EMV/2014/emv-now-seems-assured-should-u-s-payments-firms-readjust-and-stick-to-their-roots.

Henry, David. "Millions of Target shoppers face new debit card limits." Reuters.com, Dec 21, 2013. http://www.reuters.com/article/2013/12/21/us-target-jpmorgan-idUSBRE9BK0D020131221 .

Kitten, Tracy. "Target Breach: The Cost to Banks." InfoRisk Today Podcast. February 12, 2014. http://www.inforisktoday.com/interviews/target-breach-cost-to-banks-i-2182.

Krebs, Brian. "Card Backlog Extends Pain from Target Breach." Krebs on Security. February 14, 2014. http://krebsonsecurity.com/2014/02/card-backlog-extends-pain-from-target-breach/.

Krebs, Brian. "Cards Stolen in Target Breach Flood Underground Markets." Krebs on Security. December 20, 2013. http://krebsonsecurity.com/2013/12/cards-stolen-in-target-breach-flood-underground-markets/Levitin, Adam. "Debit Interchange Post-Durbin: Some Early Numbers." Credit Slips. May 1, 2012, available at http://www.creditslips.org/creditslips/2012/05/debit-interchange-post-durbin-some-early-numbers.html.

MacCarthy, Mark. "Information Security Policy in the U.S. Retail Payments Industry." Workshop on the Economics of Information Security, June 2010.

MasterCard. "Chargeback Guide." 11 December 2013. PDF available at http://www.mastercard.com/us/merchant/pdf/TB_CB_Manual.pdf.

MasterCard. "Interchange and the Durbin Amendment." Mastercard.com's "*Understanding Interchange*" section http://www.mastercard.com/us/company/en/whatwedo/interchange.html. Undated pdf available at http://www.mastercard.com/us/company/en/docs/Interchange_and_Durbin.pdf

MasterCard. "Security Rules and Procedures: Merchant Edition." 30 August 2013. PDF available at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf

MasterCard. "Transaction Processing Rules." 13 December 2013. PDF available at http://www.mastercard.com/us/merchant/pdf/TPR-Entire_Manual_public.pdf.

Morrison, David. "Interchange Suit Unlikely to Address Fraud Costs." *Credit Union Times*, January 23, 2014, available at http://www.cutimes.com/2014/01/23/interchange-suit-unlikely-to-address-fraud-costs.

Murdoch, Steven J. and Ross Anderson. "Security Protocols and Evidence: Where Many Payment Systems Fail." To be presented at Financial Cryptography and Data Security 2014, March 2014. PDF available at http://www.cl.cam.ac.uk/~sjm217/papers/fc14evidence.pdf.

Navetta, David. "VISA Phases Out the Account Data Compromise Recovery (ADCR) Process and Implements the Global Compromised Account Recovery (GCAR) Program." InfoLawGroup.com, January 9 2013, available at http://www.infolawgroup.com/2013/01/articles/uncategorized/visa-phases-out-the-account-data-compromise-recovery-adcr-process-and-implements-the-global-compromised-account-recovery-gcar-program/.

PCI Security Standards Council. "Ten Common Myths of PCI DSS." PCISecurityStandards.org, October 2010. PDF available at https://www.pcisecuritystandards.org/documents/PCI%20SSC%20-%20Ten%20Common%20Myths.pdf.

Prager, Robin A., Mark D. Manuszak, Elizabeth K. Kiser, and Ron Borzekowski. "Interchange Fees and Payment Card Networks: Economics, Industry Developments, and Policy Issues." Finance and Economics Discussion Series, Divisions of Research & Statistics and Monetary Affairs. Federal Reserve Board, Washington, D.C., 2009-23. May 13, 2009. PDF available at http://www.federalreserve.gov/pubs/feds/2009/200923/200923pap.pdf.

Quinn, Stephen and William Roberds. "The Evolution of the Check as a Means of Payment: A Historical Survey." *Federal Reserve Bank of Atlanta: Economic Review*, Number 4, 2008. PDF available at https://www.frbatlanta.org/filelegacydocs/er08no4_QuinnRoberds.pdf.

Sekar, Anisha. "The Durbin Amendment Explained." *NerdWallet Credit Card Blog*. Last updated 9/26/12, available at http://www.nerdwallet.com/blog/banking/durbin-amendment-explained/.

Sullivan, Richard J. "The Changing Nature of U.S. Card Payment Fraud: Issues for Industry and Public Policy." For presentation at the 2010 Workshop of Economics of Information Security. May 21, 2010.

Summers, Nick. "ATMs Face Deadline to Upgrade From Windows XP." *BloombergBusinessweek*, January 16, 2014, available at http://www.businessweek.com/articles/2014-01-16/atms-face-deadline-to-upgrade-from-windows-xp.

Visa. "Visa International Operating Regulations." 15 October 2013. PDF available at http://usa.visa.com/download/merchants/Public-VIOR-15-October-2013.pdf.

Visa. "Visa Global Compromised Account Recovery Program: What Every Merchant Should Know About GCAR." PDF available at http://usa.visa.com/download/merchants/what-every-merchant-should-know-GCAR-VOL-091213-final.pdf

Skeen, Dale. "How Real-Time Analytics Protects Banks from Large Scale Cyber Attacks." *Information Security Buzz*, accessed Feb 23, 2014. http://www.informationsecuritybuzz.com/real-time-analytics-protects-banks-large-scale-cyber-attacks/

Varian, Hal. "Managing Online Security Risks." New York Times; New York, N.Y.; Jun 1,2000.

Webster, Karen. "Black Swans, Payments and 1982." Pymnts.com. 10 February 2014, available at http://www.pymnts.com/briefing-room/mobile/mobile-payments/2014/black-swans-payments-and-1982.