Should Payment Card Issuers Reissue Cards in Response to a Data Breach?

James T. Graves, Alessandro Acquisti, and Nicolas Christin[1]

Abstract

Credit card issuers face a choice when card data has been exposed in a data breach but has not yet been used for attempted fraud: reissue the cards or wait until fraud is attempted. This article empirically investigates the first-order public and private costs and benefits of each of these options. Based on extrapolations of the total number of credit card records exposed in data breaches, the probability that a card exposed in a breach will be used for fraud, and the cost of fraud, the first-order costs of automatically reissuing cards seems to be higher than waiting until fraud is attempted. We also briefly discuss second-order costs that may change the results of our first-order model.

1 Introduction

Every year, millions of credit card records are exposed in data breaches.[2] When a breach is disclosed, financial institutions that issue credit cards face a choice: immediately cancel and reissue potentially affected cards, or wait until someone attempts to use the card data for fraud. Reissuing cards can be expensive, and many cards impacted in a breach will never be used for fraud. But not reissuing cards increases the risk of credit card fraud, which is also costly. Fraud-monitoring programs can prevent some fraud before it happens, but not all. Industry practice on credit card reissue after a breach has been mixed.[3] Although many issuers no doubt internally evaluate the risks and benefits of reissuing, to our knowledge no published study has attempted to measure the merits of each option when costs external to the issuers are considered.

This paper makes two contributions to the literature on data breach and identity theft. First, we address the question implied by the title of the paper: is it more expensive

[1] Carnegie Mellon University. This work was partially funded by the Department of Homeland Security (DHS) Science and Technology Directorate, Cyber Security Division (DHS S&T/CSD) Broad Agency Announcement 11.02, the Government of Australia and SPAWAR Systems Center Pacific via contract number N66001-13-C-0131 and by NSF IGERT grant DGE-0903659. This paper represents the position of the authors and not that of the aforementioned agencies.

[2] *See infra* § 3.3.1.

[3] *See, e.g.*, Maria Aspan, *Citi, B of A Cards Hit by Data Breach*, AM. BANKER, Aug. 22, 2011, at 7 (reporting that Citigroup and Bank of America reissued "some credit cards"); Maria Aspan, *Sony Breach Could Cost Card Lenders $300 Mln*, REUTERS NEWS, Apr. 29, 2011 (reporting that Bank of America and American Express were not automatically reissuing cards after the Sony data breach); Rita Trichur, *Cardholders here Caught in U.S. Security Breach*, TORONTO STAR, Jan. 30, 2009, at B1 (stating that TD Bank was not reissuing cards after the data breach of Heartland Payment Systems but would be "closely monitoring those accounts for unusual activity"); Ann Ravana, *Banks Start Credit Card Reissue*, BANGOR DAILY NEWS, Feb. 8, 2007, at 4 (reporting that Bangor Savings Bank was reissuing all cards after the TJX breach).

to society if issuers reissue credit cards or not? Second, our estimation and analysis illustrate where improved access to quality data sources is most needed.

We analyze the costs involved in reissuing cards versus not reissuing cards using an estimation of the extent to which credit cards are exposed in data breaches and data on the extent and cost of identity theft. Although the cost and sources of identity theft are well-researched, the connection between identity theft and data breach is not as well understood. We deal with this uncertainty through parameterization, the use of ranges of values, sensitivity analysis, and Monte Carlo analysis. We analyze public information about reported credit card breaches with known record counts to extrapolate an estimate of unknown records that would also have been exposed.

Our results are limited by the fact that we rely on publicly available information about data breach and identity theft. Some of this information, particularly the information about identity theft compiled by the Department of Justice's Bureau of Justice Statistics, is excellent. Other data, such as estimates of the percentage of existing-account credit card fraud attributable to data breach, are not. The extent to which our model is sensitive to different data sources may serve as a guide for where resources could most usefully be spent to improve understanding of the causes of data breach.

Part 2 discusses the structure of the payment card system in the United States and related research. Part 3 describes the methodology and the data used. Part 4 presents the analysis of the data. Part 5 briefly discusses some additional economic factors, which we refer to as "second-order effects," that may affect the costs involved in an issuer's decision whether to reissue. Part 6 lists some of the limitations of this research, and Part 7 concludes.

2 Background

Credit card payments rely on relationships between five parties: cardholders, merchants, issuing banks, acquiring banks, and card associations.[4] An acquiring bank (or "acquirer") is the merchant's bank; the issuing bank (or "issuer") is the bank with whom the cardholder has a revolving credit account. The card associations (e.g., MasterCard, Visa, American Express, or Discover) are networks of financial institutions that set rules governing transactions. In the case of American Express and Discover, the card network and issuer are usually the same.

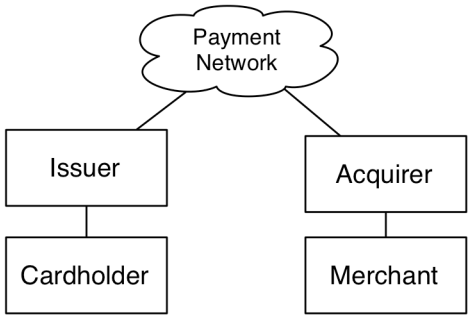

Figure 1: Credit card network structure

In simplified form, a credit card transaction works as follows. When a cardholder presents a card for payment at a merchant, the merchant passes the card information and authorization request to its acquiring bank, which forwards the

[4] Adam J. Levitin, *Private Disordering? Payment Card Fraud Liability Rules*, 5 Brook. J. Corp. Fin. & Com. L. 1, 10 (2010).

request to the cardholder's issuing bank. The issuer authorizes or rejects the transaction. If the transaction is authorized, the issuer transfers funds from its payment network account to the acquirer's payment network account. This is called "capture." Finally, the transaction is "settled" when the acquirer credits the merchant's account. [5]

In the United States,[6] issuers bear the initial risk of loss from credit card fraud from card-present transactions, but the contractual relationships between issuers, the card brands, merchants, and the merchants' acquiring banks allow those losses to be shifted to merchants that have violated the card brand Operating Regulations by not following prescribed security measures.[7] In most states, however, loss-shifting is available only for fraudulent charges.[8] Issuers bear all the operational costs of reissuing cards,[9] and have had little success in lawsuits to recoup these costs from breached merchants.[10] But issuers who sue cannot recover damages they could have avoided.[11] If an issuer could have reduced fraudulent charges to an exposed card by canceling and reissuing that card but did not, the issuer may not be able to recover the cost of those charges if they could have been avoided. Conversely, if the total amount of fraudulent charges that result from a breach are lower than the cost of reissuing the cards, reissuing would be failing to mitigate damages.

In at least one case, merchants have used the fact that an issuer reissued cards and lacked fraud monitoring processes to claim that issuers did not mitigate damages. In the consolidated putative class-action lawsuit resulting from the breach at TJX, one of the retailer's defenses was that by "unnecessarily and unreasonably automatically canceling and reissuing their customers' debit cards in response to the data compromise" and by not using

---

[5] *Id.* at 10-12.

[6] This paper focuses on the credit card systems in the United States, where federal law limits consumer liability for unauthorized credit and debit card charges. *See* 15 U.S.C. § 1643(a)(1)(B) (setting maximum consumer liability for unauthorized credit card use at $50); 12 C.F.R. § 226.12(b) (same); 15 U.S.C. § 1693g(a) (limiting consumer liability for debit cards to $50 as long as loss is reported within two business days); 12 C.F.R. § 205.6(b) (same).

[7] *See* Pa. State Employees Credit Union v. Fifth Third Bank, No. 1:CV-04-1554, 2006 WL 1724574, at *2–*5 (M.D. Pa. June 16, 2006) (describing the provisions of Visa's Operating Regulations); Levitin, *supra* note 4, at 15 (2010).

[8] Minnesota and Washington State have statutes allowing issuers to recover the costs of reissuing cards in some circumstances. *See* MINN. STAT. § 325E.64 (2012) (creating a private cause of action for issuers who reissue cards as a result of an organization retaining full-track payment card data); WASH. REV. CODE § 19.255.020 (creating a cause of action for the cost of reissuing payment cards against any business that is breached because it "fail[ed] to take reasonable care to guard against unauthorized access").

[9] *Pa. State Employees Credit Union v. Fifth Third Bank*, 2006 WL 1724574 at *5.

[10] *See, e.g.*, Pa. State Employees Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 338 (M.D. Pa. 2005); Pa. State Employees Credit Union v. Fifth Third Bank, No. 1:CV-04-1554, 2006 WL 1724574, at *1 (M.D. Pa. June 16, 2006) (dismissing third-party beneficiary claims that remained after the court had granted a motion to dismiss on all other claims).

[11] The doctrine of avoidable consequences (sometimes erroneously referred to as a "duty to mitigate" damages) is a doctrine in tort and contract law that prevents a plaintiff from recovering damages he or she could have avoided with reasonable effort. Restatement (Second) of Torts § 918(1) (1979); Restatement (Second) of Contracts § 350 (1981); *see also* 3 JACOB A. STEIN, STEIN ON PERSONAL INJURY DAMAGES § 18:1 (2008).

fraud monitoring, some of the plaintiffs had either failed to mitigate damages or were contributorily negligent.[12] Too much should not be read into these claims, however. It is common practice for plaintiffs to pursue every plausible legal theory; only a judgment on the merits can prove whether those theories are valid.[13]

The extent of data breach and, separately, credit card fraud have been the subjects of extensive study. For several years, the Federal Trade Commission published an annual identity theft survey report[14] and still publishes annual reports on complaints to the Consumer Sentinel Network.[15] The Bureau of Justice Statistics includes questions about identity theft in its annual National Crime Victimization Survey.[16] As discussed later in this work, a few organizations try to track the extent of data breach.[17] In the academic arena, Ross Anderson et al. conducted a systematic study of the cost of cybercrime.[18] Acquisti, Friedman, and Telang found that data breaches negatively affected stock prices.[19]

The economics of security investment, breach, and identity theft have also been fertile research areas. Gordon and Loeb developed an economic framework to describe the optimal amount an organization should spend to protect data.[20] Romanosky, Telang, and Acquisti studied whether data breach laws reduce identity theft.[21] They found evidence that the laws did reduce identity theft, but by a small amount. Estimating the impact of breaches is particularly challenging given the unknowns. Thomas et al. recently applied a branching activity model to the problem.[22]

---

[12] Answer to Plaintiffs' Consolidated Class Action Complaint at 22, *In re* TJX Retail Security Breach Litigation, 527 F.Supp.2d 209 (D. Mass. 2007) (No. 07-10162-WGY), 2007 WL 5324216.

[13] TJX raised twenty-six affirmative defenses in its answer to the class-action suit, *id.* at 18–23, and the suit was settled without resort to these defenses. *TJX, Banks Settle Data Breach Lawsuit*, BOSTON GLOBE, Sept. 3, 2009, at 6.

[14] *See, e.g.,* SYNOVATE, FEDERAL TRADE COMMISSION—2006 IDENTITY THEFT SURVEY REPORT (2007), *available at* http://www.ftc.gov/reports/federal-trade-commission-2006-identity-theft-survey-report-prepared-commission-synovate

[15] *See* FTC, CONSUMER SENTINEL DATA BOOK FOR JANUARY–DECEMBER 2013 (2014), *available at* http://www.ftc.gov/enforcement/consumer-sentinel-network/reports.

[16] *See* LYNN LANGTON, BUREAU OF JUSTICE STATS., PUB. NO. NCJ 236245, IDENTITY THEFT REPORTED BY HOUSEHOLDS, 2005-2010 (2011) [hereinafter BJS 2011].

[17] *See infra* § 3.3.1.

[18] Ross Anderson et al., *Measuring the Cost of Cybercrime*, *in* 12th WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS) (2012).

[19] Alessandro Acquisti, Allan Friedman, and Rahul Telang, *Is There a Cost to Privacy Breaches?* FIFTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS) (2006).

[20] Lawrence A. Gordon and Martin P. Loeb, *The Economics of Information Security Investment*, 5 ACM TRANSACTIONS ON INFORMATION AND SYSTEM SECURITY 438 (TISSEC).

[21] Sasha Romanosky et al., *Do Data Breach Disclosure Laws Reduce Identity Theft?*, *in* SEVENTH WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS) (2008).

[22] Russell Thomas et al., *How Bad Is It? – A Branching Activity Model to Estimate the Impact of Information Security Breaches*, 12th WORKSHOP ON THE ECONOMICS OF INFORMATION SECURITY (WEIS) (2013).

3 Methodology and Data

3.1 Cost Model

We are interested in the aggregate social costs of the decision faced by credit card issuers: those costs incurred by anyone affected by the issuer's decision. We categorize those costs as "first order" costs or "second order" costs.

We use the term "first-order costs" to describe those costs that are proximate results of reissuing cards or leaving them in circulation despite possible compromise. First order costs include the direct costs to issuers, merchants, and consumers of reissuing credit cards. These include mailing costs, issuer overhead costs attributable to reissuing cards, time spent by merchants and consumers responding to having cards reissued, etc. We also include the cost of fraud as a first-order cost, since the possibility of fraud is the most obvious risk of not reissuing cards.

We call costs that the reissuance decision more indirectly brings about "second-order costs." For example, whether or not an issuer cancels potentially compromised cards could affect the incentives cybercriminals have to steal credit card data. Most of this paper focuses on first-order costs, but in Part 5 we briefly discuss second-order costs.

To estimate the first-order costs of reissuing cards, we determine the cost to the main parties involved in card transactions—cardholders, issuers, and merchants—if cards are reissued versus if they are not. Costs related to canceling and replacing the cards themselves are different for each of these three parties, and should be considered separately. The cost of fraud can be treated as an overall cost instead of trying to determine who bears fraud losses. Because the model considers aggregate social costs, who incurs the cost of fraud is less critical to the model than is the total amount of that fraud.

We use the following model to represent this approach to calculating the first-order costs:

$$\sum_{k}(r(c_{i_k} + c_{h_k} + c_{m_k}) + (1 - r)\rho_k f_k) \tag{1}$$

The formula sums, over each affected account k, the costs related to that account, where $r = 1$ if the cards associated with an account are reissued and $r = 0$ if not. We represent the costs of reissue by c_{i_k} for the issuer i_k of account k, c_{h_k} for the account holder h_k, and c_{m_k} for merchants processing payments to account k. These terms capture only the direct costs (whether monetary or in terms of time or other resources) of canceling and replacing cards for each account, not the cost of the cards being used fraudulently.

The cost of fraud is entirely contained within the $\rho_k f_k$ term. The term ρ_k is the probability that account k will be used fraudulently. The term f_k is the amount of fraud if the account is used fraudulently. This term is not broken down between cardholder, issuer, and

merchant because we are interested in the aggregate societal costs. This representation of the model includes the assumption that fraud losses are zero if cards are reissued.[23]

Our estimation focuses on whether, in the United States, the expected societal cost of existing-account credit card fraud if cards are not reissued after a breach is greater than the societal cost of reissuing credit cards. This statement includes some important details. First, we concentrate on credit cards, not debit cards or other payment instruments because debit cards have different authentication structures and risk profiles from credit cards and thus should be distinguished from credit cards when analyzing the costs from breach. Second, our analysis is specific to the United States because the legal and technical environment for payment cards is quite different outside the United States. Third, we concentrate on overall societal costs, not the allocation of those costs between parties. Fourth, we focus specifically on existing-account credit card fraud as the primary cost of credit card fraud. This is a subtype of identity theft—one in which victims' existing credit cards are used for unauthorized charges. Credit card data is unlikely to facilitate other forms of identity theft such as new-account fraud (in which new accounts are opened using the victim's identity).[24]

Note also that the cost of reissuing is primarily a per-*card* cost. Each physical card must be printed and mailed, for example. But the cost of existing-account credit card fraud depends largely on the number of *accounts* affected in a breach, not the number of individual cards those accountholders have.

3.2 The Cost of Reissuing Cards

Our calculations of the cost of reissuing cards rely on the simplifying assumption that merchants and cardholders incur no significant non-fraud costs when cards are reissued. A canceled and reissued credit card used for recurring payments may lead to a merchant having to contact customers to obtain new payment information, but these processes are generally automated and inexpensive.[25] The costs to cardholders come from the value of time spent responding to the cancelation—for example, updating auto-pay accounts to use the new card number. Issuers usually minimize these costs by sending replacement cards before canceling outstanding cards, but cardholders do sometimes miss or ignore the payment cards or are traveling when the replacements are made.[26]

---

[23] It may still be possible to use canceled cards fraudulently if a merchant is not vigilant about clearing authorization before goods or services have been rendered. We assume that the overall loss from these pre-authorization transaction losses is negligible.

[24] *See* Lynn Langton & Michael Planty, Bureau of Justice Stats., Pub. No. NCJ 231680, Victims of Identity Theft, 2008, at 2 (2010).

[25] *See, e.g.*, Authorize.net, Pricing, http://www.authorize.net/solutions/merchantsolutions/pricing/ (listing an authorization fee of $.10 per authorization request) (last visited Jan. 1, 2013); Merchant Warehouse, Glossary, Authorization Fee, http://merchantwarehouse.com/glossary/authorization-fee (stating that "[t]he average cost in the United States for an authorization is five to ten cents per transaction, but can be as high as twenty-five cents or more") (last visited Jan. 1, 2013).

[26] *See, e.g.*, Eric Stark, *Computer Hackers Are Stealing Bank Card Information, But There Is Protection and Some Banks Have Been Aggressive*, SUNDAY NEWS (Lancaster, Pa.), July 11, 2004, at 1 (describing the situa-

By omitting possible costs to merchants and cardholders of reissuing cards, our analysis errs on the side of underestimating the cost of reissuing cards.

A number of different expenses factor into issuers' cost of reissuing cards. Printing the cards is one such expense, which may vary based on whether the cards are personalized or contain features like a photograph of the cardholder. Mailing the cards is another expense. Some other expenses could be considered "overhead." For example, an issuer might have to budget for extra customer service expenditures to answer questions about reissued cards. Card account information would need to be updated in the issuer's database if cards are reissued with new numbers.

Estimates of the cost of reissuing cards range from $3 to $25 per card. Table 1 lists some estimates of the cost of reissuing cards. The first six entries list estimates taken directly from surveys or from bank estimates or calculated from costs they alleged. For example, Pennsylvania State Employee's Credit Union (PSECU) alleged in court filings that it canceled about 20,000 cards at a total cost of $100,000.[27] The state of Maine also conducted a survey of credit card issuers in the state after large-scale breaches at TJX and Hannaford. The remaining five entries are estimates by analysts or unnamed issuers.

We use a per-card reissue cost for simplicity but recognize that reissuing costs may benefit from economies of scale. Indeed, among the estimates derived from actual reissues, issuers who reissued larger numbers of cards seem to have incurred lower per-card costs. The issuers in the $5–$6 per card range reissued 20,000 (PSECU and Fulton Bank) and 81,000 cards (Sovereign Bank). The higher numbers were based on reissuing 71 (Merrill) and 4,000 cards (TrustCo). One might surmise that the "top issuer" cited by the Aite Group has enough cardholders for its per-card reissuing costs to drop into the $3–$5 range. It is also possible, however, that cost figures based on interviews do not distinguish between the costs of physically reissuing the cards (pressing new plastic, mailing the cards, etc.) and overhead in the reissuing process.

We assume that the cost of reissuing a card is therefore about $3–$25 per card. We believe that for most issuers, the cost is between $5–$10 per card but the per-card cost is higher in some cases. To obtain a per-account cost of reissuing cards, we simply multiply by the ratio of cards to accounts, which is about 1.2.[28] That leads to an estimated cost of $3–$31 per account.

3.3 The Cost of Not Reissuing Cards

Calculating the cost of not reissuing cards is much less straightforward. The calculation may be simple, but the values needed for those calculations are subject to quite a bit of uncertainty.

---

tion of a cardholder who discovered in a checkout line that her debit card had been deactivated due to a reissued card).

[27] Interestingly, even though plaintiffs in a lawsuit have incentives to inflate their damage claims, PSECU's claimed cost of $5 per card is at the lower end of cost estimates.

[28] *See* NILSON REPORT, November 15, 2008, at 10 (listing 1,254,000 general-use credit cards outstanding on 1,041,000 accounts).

Table 1: Estimates of the cost per card to reissue credit cards

Source or Issuer	$/card
Maine survey of issuers[29]	$4.72
Penn State Employees Credit Union[30]	$5
Fulton Bank[31]	$5
Sovereign Bank[32]	$6
Merrill Bank[33]	$14
TrustCo Bank[34]	$20
Reuters ("several analysts")[35]	$3–$5
Aite Group ("according to one top issuer")[36]	$3–$5
Gartner[37]	$10
"Various banks and credit unions"[38]	$5–$25
America's Community Bankers[39]	$10–$20

[29] ME. BUREAU OF FIN. INST., MAINE DATA BREACH STUDY 18–20, Nov. 24, 2008, available at http://www.state.me.us/pfr/financialinstitutions/reports/index.htm. The study also showed a net cost of fraud per card of $4.80 on average. *Id.*

[30] Pa. State Emps. Credit Union v. Fifth Third Bank, 398 F. Supp. 2d 317, 322 (2005) (stating that PSECU canceled 20,029 cards at a total cost of $98,128.13).

[31] Eric Stark, *Computer Hackers are Stealing Bank Card Information, but There Is Protection and Some Banks Have Been Aggressive*, SUNDAY NEWS (Lancaster, Pa.), July 11, 2004, at 1 (reporting that Fulton Bank spent $100,000 to replace 20,000 cards).

[32] Mark Jewell, *IDs Are a Steal; Thieves Looking for Credit Numbers Set Their Sights on Big Targets*, COLUMBIAN (Vancouver, WA), Aug. 23, 2004, at E (reporting that Sovereign Bank reissued 81,000 cards twice at a total cost of $1 million).

[33] Ann Ravana, *Banks Start Credit Card Reissue*, BANGOR DAILY NEWS, Feb. 8, 2007, at 4 (quoting Merrill Bank Senior Vice President Lynne Spooner as saying that the cost of replacing 71 cards was about $14 per card).

[34] Chris Churchill, *TJX Reacts to Bank Lawsuit: T.J. Maxx Parent in Filing Says TrustCo Failed to Mitigate Injury from Data Breach*, TIMES UNION (Albany, N.Y.), Aug. 30, 2008 (quoting that TrustCo as saying that its cost to replace 4,000 debit cards after the TJX breach was $20 per affected account).

[35] Maria Aspan, *Sony Breach Could Cost Card Lenders $300 Mln*, REUTERS, Apr. 29, 2011, *available at* http://www.reuters.com/article/2011/04/28/sony-creditcards-cost-idUSN2826485220110428 (reporting that "[e]ach customer request to replace a credit card would cost lenders about $3 to $5 per card," which includes "the new piece of plastic itself, postage, and various customer service costs").

[36] SHIRLEY W. INSCO, AITE GRP., GLOBAL CONSUMERS REACT TO RISING FRAUD: BEWARE BACK OF WALLET (2012), *available at http://www.aciworldwide.com/~/media/Files/Collateral/ACI_Aite_Global_Consumers_React_to_Rising_Fraud_1012* ("According to one top issuer, it costs between US$3 and US$5 to issue a replacement card.").

[37] Andrew Johnson, *Card Fraud Risk Low From Breach at Citi*, AM. BANKER, June 10, 2011, at 10 (reporting a Gartner analyst's "rough estimate" that it would cost Citigroup about $10 per card to replace cards after a data breach).

[38] Denis Paiste, *Compromised Credit Cards top 100,000*, N.H. UNION LEADER, Jan. 31, 2007, at B3 (reporting that "Various banks and credit unions have said it costs from $5 to $25 per card reissued").

[39] *ACB Data Breach Survey Highlights Need for Action by Card Networks and Congress*, PR NEWSWIRE, Feb. 7, 2007, http://www.prnewswire.com/news-releases/acb-data-breach-survey-highlights-need-for-action-by-card-

We assume that the vast majority of issuers already use some form of fraud monitoring. This has two implications. First, the marginal cost to monitor a card that has been exposed in a data breach is essentially zero. An issuer might flag a card in its fraud-monitoring system, which would mark the card as potentially exposed and could trigger additional protections, but changing a database variable has negligible marginal cost if the database is set up to accommodate such a flag. Second, this assumption implies that the current level of existing-account credit card fraud already reflects the use of fraud monitoring and prevention systems. Flagging a card might improve the probability that attempted fraud will be detected and prevented—at some risk of additional false positives—but the baseline probability of fraud does not rely on the effectiveness of current fraud-monitoring processes.

The cost of not reissuing a card therefore boils down to the expected cost of fraud on that account, $\rho_k f_k$. High-quality statistics are available on the number of *households* victimized by existing-account credit card fraud each year. But ρ_k in our model is the probability that an *account* will be used for existing-account credit card fraud. We therefore start with the probability that a household will experience existing-account credit card fraud (call this ρ_h) and convert that to a per-account probability.

If a household has a credit card accounts, the probability that a household experiences fraud on at least one of them is:

$$\rho_h = 1 - (1 - \rho_k)^a \tag{2}$$

We can estimate the probability that a particular *household* will experience existing-account credit card fraud as vb/n, where n is the number of credit card records exposed in data breaches annually, v is the number of households victimized by existing-account credit card fraud each year, and b is the percentage of all existing-account credit card fraud in which the source of the card information was a data breach. To convert to a per-account probability of fraud, we substitute $\rho_h = vb/n$ in equation (2) and solve for ρ_k to get the following:

$$\rho_k = 1 - \left[1 - \frac{vb}{n}\right]^{1/a} \tag{3}$$

Note that this calculation assumes that the card numbers exposed in breaches are unique—i.e., that two different breach events do not expose the same credit card number. Overlap between breaches would reduce the total number of credit card numbers exposed. This assumption seems reasonable given the current common (if not universal) practice of reissuing credit cards potentially exposed in a breach.

---

networks-and-congress-54632297.html (claiming that "cumulative data reflect that the average cost for reissuing each debit card is approximately $10-20 per card"). The survey referenced in the press release does not appear to be available.

The calculations also use annual averages. As will shortly be discussed, the number of cards exposed in data breaches varies widely from year to year. Using annual averages reflects the assumption that both collection and misuse of credit cards occurs over time. Although a massive breach may be announced on a certain date, access to the data may have occurred over weeks or months. Thus, it seems to make sense to smooth this data by considering annual averages and not focusing on individual yearly totals.

3.3.1 The Number of Credit Card Records Exposed in Data Breaches

The number of records exposed in data breach is uncertain, for three reasons. First, the only breaches that can be counted are those that are discovered. Undetected breaches are by their very nature impossible to count unless they are eventually discovered. Second, not all breaches that are discovered are publicly disclosed. Although forty-six states and the District of Columbia now have laws requiring organizations to notify data subjects when their information has been exposed,[40] most of the laws do not require the breaches to be publicized or reported to a public official. Third, even when a breach has been detected and reported, it may not be possible to determine how many records were exposed. In some cases, a breached organization can offer only a rough estimate of the number of records that might have been compromised.

Three major sources track nationwide data breaches.[41] The Privacy Rights Clearinghouse (PRC) maintains a searchable and downloadable breach database compiled from various publicly available sources.[42] The Identity Theft Resource Center (ITRC) also tracks publicly-reported data breaches and publishes lists of breaches and statistics.[43] ITRC's data is not available for download except as PDF reports. The third source is Verizon's RISK Team, which publishes an annual Data Breach Investigations Report (DBIR) based on data obtained from incidents investigated by Verizon, the U.S. Secret Service, and police and cybercrime units from other countries.[44] The PRC and ITRC col-

---

[40] *See* James T. Graves, Note, *Minnesota's PCI Law: A Small Step on the Path to a Statutory Duty of Data Security Due Care*, 34 WM. MITCHELL L. REV. 1115, 1118 (2008) (listing data breach laws in thirty-nine states and the District of Columbia). Since the publication of that article, Alaska, Iowa, Mississippi, Missouri, Oregon, Virginia, and West Virginia have also enacted breach laws, bringing the total to forty-six. *See* ALASKA CODE §§ 45.48.010–.090; IOWA CODE §§ 715C.1–.2; MISS. CODE ANN. § 75-24-29 (2012); MO. REV. STAT. § 407.1500; OREGON REV. STAT. §§ 646A.600–.604; VA. CODE § 18.2-186.6, § 32.1-127.1:05; W. VA. CODE §§ 46A-2A-101 to -105. The four states without data breach notification laws as of this writing are Alabama, Kentucky, New Mexico, and South Dakota.

[41] The web site datalossdb.org also compiles a database of data breaches. Because access to the datalossdb.org data "requires authorization and potential licensing arrangements," we do not consider it to be a public information source and did not use it for this study.

[42] *See* Privacy Rights Clearinghouse, Chronology of Data Breaches, 2005–Present, http://www.privacyrights.org/data-breach (last visited Dec. 20, 2012).

[43] *See* Identity Theft Resource Center, Data Breaches, http://www.idtheftcenter.org/artman2/publish/lib_survey/ITRC_2008_Breach_List.shtml (last visited Dec. 29, 2012).

[44] *See* VERIZON ENTER. SOLUTIONS, 2012 DATA BREACH INVESTIGATIONS REPORT (2012), *available at* http://www.verizonbusiness.com/about/events/2012dbir/ [hereinafter VERIZON DBIR 2012].

lect and report information on data breaches in the United States; Verizon's 2012 report includes data on breaches in twenty-two countries.[45]

Table 2: Data breach record counts reported by the Privacy Rights Clearinghouse (PRC), Identity Theft Resource Center (ITRC), and Verizon (millions of records)

	PRC			ITRC		Verizon	
Year	Total Recs	Pmt cards	CC Breach Events	Total Recs	Pmt cards	Total Recs	Pmt cards
2006	48.6	4.0	52 (38)	19.1		124.2	
2007	130.3	109.0	55 (35)	127.7		171.0	
2008	49.7	7.2	43 (21)	35.7		360.8	279.7
2009	218.9	130.8	27 (12)	222.5		143.6	119.2
2010	12.9	1.2	87 (40)	1.2		3.9	3.7
2011	66.1	13.7	103 (58)	22.9	3.4	174.5	5.2
2012	27.1	7.7	90 (33)	17.0	4.4		
Total	553.7	273.6	457 (237)	446.4		978.1	
Avg/yr	79.0	39.1	65 (34)	74.4		163.0	

Sources: (1) Privacy Rights Clearinghouse, [46] (2) Identity Theft Resource Center,[47] (3) Verizon[48]

Notes: Total records are the number of records exposed according to each source. PRC "Payment cards" column shows PRC's estimate for the number of records potentially exposed in breaches that PRC described as involving unencrypted full payment card numbers. "CC Breach Events" counts the number of breach events (as opposed to records) that the PRC described as involving unencrypted full payment card numbers; the number of those breach events for which a record count could be estimated is given in parentheses. The ITRC only began reporting payment card numbers as a separate category in 2011. The Verizon "Total Records" column lists the number of records exposed per year in breaches investigated by Verizon and the U.S. Secret Service. The Verizon "Payment cards" column shows the number of payment cards exposed these breaches as calculated from a percentage of all breaches that exposes payment cards (as reported by Verizon). The 279.7 million records listed for 2008 is based on 98% of the 285.4 records Verizon investigated in that year; Verizon's later reports updated the total number of records investigated by Verizon and the Secret Service to 360.8 million but did not indicate how many of those records were payment card numbers. Figures for 2012 are annualized estimates based on year-to-date figures as of December 20, 2012 for PRC and June 30, 2012 for ITRC.

[45] VERIZON DBIR 2012, *supra* note 44, at 12.

[46] Privacy Rights Clearinghouse, Chronology of Data Breaches, 2005–Present, http://www.privacyrights.org/data-breach (last visited Dec. 20, 2012).

[47] Identity Theft Resource Center, Data Breaches, http://www.idtheftcenter.org/artman2/publish/lib_survey/ ITRC_2008_Breach_List.shtml (last visited Dec. 29, 2012). The total number of exposed records for each year are from that year's ITRC Breach Report. *See, e.g.*, IDENTITY THEFT RES. CTR., ITRC BREACH REPORT 2010 FINAL, http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Report_20101229.pdf (2010).

[48] VERIZON ENTERPRISE SOLUTIONS, 2012 DATA BREACH INVESTIGATIONS REPORT (2012), *available at* http://www.verizonbusiness.com/about/events/2012dbir/.

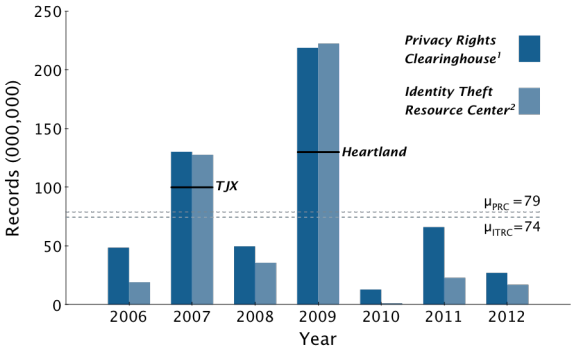

Figure 3: Estimates of breached data records by year, 2006–2012

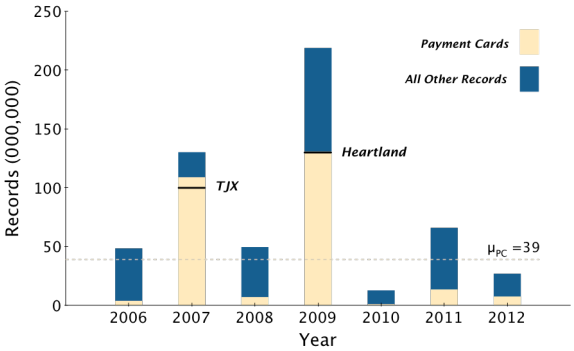

Figure 2: Credit card account records as a portion of all records breached by year, 2006–2012 (Privacy Rights Clearinghouse)

Table 2 and Figure 3 illustrate the variation in the data by year and by tracking organization. The PRC and ITRC numbers are in rough agreement, although many differences exist due either to different breaches included by each or different estimates of the number of records affected.[49] Figure 2 illustrates the number of credit cards breached per year as a proportion of all records according to the PRC. The ITRC only began reporting the statistics for exposed debit and credit cards in 2011.

The Verizon DBIR numbers, although not directly useful for calculating U.S. data breach statistics, are interesting for two reasons. First, because the Verizon reports are based on data from multiple countries, they provide a glimpse into the worldwide data breach problem (Verizon estimates that 1 billion records have been exposed since it began recording breach data in 2004).[50] Second, the Verizon reports are based on the number of breaches investigated by Verizon and thus have a different bias than publicly reported breaches. Some of the data used by Verizon is not publicly available. At the same time, Verizon's reports are biased toward the types of large breaches for which organizations call in professional investigation help.[51]

More striking is the variation in estimated record count year to year. Much of this variation is the result of only two breaches: the TJX breach, disclosed in 2007, which exposed an estimated 100 million payment card records, and the 2009 Heartland Payment Systems breach that compromised about 130 million cards.[52] Excluding these two breaches

[49] The Global Payments breach announced on March 30, 2012 is one example of how the PRC and ITRC report uncertain record counts differently. Global Payments announced that some of its payment servers had been compromised, potentially exposing full-track payment card data for 1.5 million accounts. In May, it announced that it had discovered that the breach had been going on longer than it had previously believed and that up to 7 million accounts may have been exposed although it continued to believe that only 1.5 million records had been affected. The PRC database attributes 7 million exposed records to the breach; ITRC's uses the 1.5 million number.

[50] *See* VERIZON DBIR 2012, *supra* note 44, at 45.

[51] *See id.* at 8 (discussing bias).

[52] Both of these breaches were the work of one ringleader: Albert Gonzalez, who was convicted in federal court of masterminding not only the TJX and Heartland breaches but several other breaches that had not

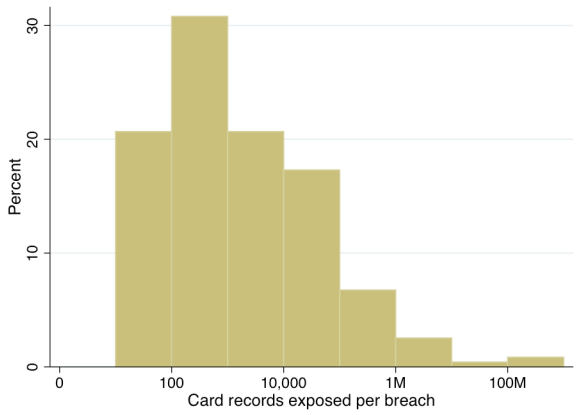

Figure 4: Distribution of payment cards exposed per breach according to the PRC database (n=237)

would lower both the average and standard deviation of the number of estimated payment card records affected per breach by an order of magnitude—from about 1.2 million to 180,000 and the standard deviation from about 10.7 million to 1.1 million.

Figure 4 shows the distribution of records exposed per breach according to the PRC database. More than half of all breaches with disclosed record counts exposed fewer than 1,000 payment card records. Almost a fifth exposed fewer than 100.

In Table 2, "Total Recs" lists the number of records of all types thought to have been exposed in data breaches where an estimate was given. These record types include any kind of personally identifiable sensitive data such as Social Security numbers, health information, and financial records.

The record count is based on a detailed analysis of the PRC database. We calculated the number of payment cards potentially exposed by downloading the PRC database, filtering based on the use of the word "card" in the description field, and manually categorizing each entry, based on its description, as either having potentially exposed full unencrypted payment card numbers or not. Thus, breach events that were described as having exposed only partial or encrypted payment card numbers were not included. Where necessary, the record count was updated to reflect only the number of payment cards believed to have been exposed. For example, the South Carolina Department of Revenue breach exposed tax records including about 5.4 million Social Security numbers, 3.3 million bank accounts, and 388,000 credit and debit card numbers, of which only 16,000 were unencrypted. We counted this as 16,000 exposed payment cards.[53]

An additional but important challenge is distinguishing the impact of breached *credit* cards from breached *debit* cards. In the United States, credit cards are typically signature-authorized; debit cards may be authorized by signature or PIN. Cardholder liability rules are slightly different. Use of the two types of cards is also different: credit cards tend to be used for larger purchases than debit cards.[54]

---

been disclosed. *See* James Verini, *The Great Cyberheist*, N.Y. TIMES, Nov. 10, 2010 at magazine 44, *available at* www.nytimes.com/2010/11/14/magazine/14Hacker-t.html.

[53] *See* Andrew Shain, *"For $25,000, We Wouldn't Be Here,"* CHARLOTTE OBSERVER (N.C.), Nov. 29, 2012, available at http://www.charlotteobserver.com/ 2012/11/28/3694394/for-25000-we-wouldnt-be-here.html; Privacy Rights Clearinghouse, Chronology of Data Breaches, South Carolina Department of Revenue, http://www.privacyrights.org/data-breach-asc?title=south+carolina+department+of+revenue.

[54] The average amount per transaction was $38 for debit cards and $89 for credit cards in 2009. U.S. CENSUS, 2012 STATISTICAL ABSTRACT OF THE UNITED STATES t.1184 (2012).

Table 3: Credit card records as a percentage of all cards breached by year (millions)

Year	Breached Payment cards	Total Credit Cards	Total Debit Cards	Credit Card %	Breached Credit Cards
2006	4.0	1,244	313	80%	3.2
2007	109.0	1,254	398	76%	82.7
2008	7.2	1,215	449	73%	5.1
2009	130.8	1,046	466	69%	90.5
2010	1.2	1,184	481	71%	0.8
2011	13.7	1,066	540	66%	9.1
2012	7.7	1,011	484	67%	5.2
Total	273.6			72%	191.3
Avg/yr	39.1				27.3

Source: U.S. Census, Statistical Abstract of the United States, 2012 t.1187, t.1188, 2011 t.1186, t.1187, 2010 t.1150, t.1151, 2009 t.1147, t.1148.

Note: Total Credit Cards are the number of credit cards held excluding oil cards, Universal Air Travel Plan (UATP) cards, car rental cards, phone cards, and other miscellaneous cards not likely to be used outside of their particular contexts. Debit Cards are the number of bank debit cards, which includes Visa and Master

To estimate the number of credit cards exposed in breaches, we used year-by-year census data on the number of cards held by cardholders. See Table 3. For each year, we estimated the percentage of all breached payment cards that were credit cards based on the overall percentage of payment cards that were credit cards that year.[55] We used this to calculate an estimate of the overall percentage of breached payment cards that were credit cards. This overall percentage is included as part of the model.

Note that the actual card account information held may not have the same distribution as the overall distribution of credit and debit cards. As mentioned above, credit cards have higher per-transaction values than debit cards. It is likely, therefore, that the proportion of a breached organization's payment cards that are credit cards is correlated with the average transaction size at that organization. Put another way, breaches from more expensive stores (e.g., electronics retailers) are likely to include more credit cards as a proportion of their payment cards than breaches from less expensive stores (e.g., grocery stores and restaurants).

Record counts are unknown for about half of the breach events reported in the PRC database. To estimate the total number of records exposed (and thus the probability that a payment card exposed in a breach will be used for existing-account card fraud), we extrapolated the number of records affected as shown in Table 4. Given the amount of variance in breach numbers, it makes little sense to extrapolate based on the overall average.

[55] Note that we use the number of *cards* for this calculation, not the number of *accounts*, under the assumption that accounts with multiple cardholders are used more often than accounts with only one cardholder and thus appear more frequently in breaches.

Table 4: Record counts for credit card records exposed in data breach by type of breach with extrapolation to breaches with unknown record counts (thousands of records)

Type	Breaches w/ Record Estimate	Credit Record Count	Mean	StdDev	Breaches w/ Unknown Record Ct.	Est. Record Count
Card (other)	7	63	13	28	9	114
Discarded data	22	2,793	133	483	5	665
Hacking	127	19,160	171	918	81	13,857
Insider	23	30	2	6	41	70
Physical loss	19	23	2	3	21	37
Stolen portable device	23	1,043	52	84	8	417
Card skimming	39	39	1	3	0	0
Stolen stationary device	9	397	50	84	3	149
Unknown	7	3	.5	.5	9	4
Total	276	23,538	101	654	177	15,313
Average per year	39	149			25	2,188

Notes: Data excludes the TJX and Heartland data breaches, both in the hacking category, which total an estimated 166 million credit card records, and insider breaches at Fidelity/Certify and Compass Bank, totaling an estimated 7 million records. Totals are rounded.

Instead, we calculated a weighted estimate based on the typical number of records exposed for each type of data breach. Table 4 lists the breach statistics from the PRC database by type of breach, excluding the TJX and Heartland breaches and two exceptionally large insider breaches. The TJX and Heartland breaches are excluded because we believe it unlikely that any of the breaches with unknown record counts exposed records on the order of the hundreds of millions of records exposed in those two breaches. We excluded the two insider breaches, at Fidelity and Global Payments, because they appear to be outliers: the millions of records compromised in those two breaches were three orders of magnitude larger than the average of other insider breaches with known record counts.

The weighted average extrapolates that the 177 breaches with unknown record counts from 2006 through 2012 have exposed about 15 million credit cards, or about 2.2 million per year. This estimate still may be too high, since it includes in the basis of its extrapolation five other breaches in which at least a million records were believed to have been affected. Excluding these breaches eliminates another 36.4 million records and leads to a weighted estimate of about 540 thousand records per year from unreported breaches.

We chose a point estimate of 2.9 million unknown breached records per year to allow for some likelihood of larger breaches of the type we excluded from our extrapolation. But the range we use is wide—150,000 to 7.5 million cards per year—because of the uncertainty surrounding the number of records in breaches for which record counts were not disclosed.

Another adjustment for uncertainty in the number of card records exposed in breach is to account for the number of breaches that are not detected. Unfortunately, there is no way to know how many breaches are unknown. It is necessary to make an assumption. For purposes of this analysis, we assume that undetected breaches expose 34% as many records as are exposed in detected breaches, with an upper bound of twice the number of

records. We include this as a parameter in the model. Increasing that factor to a larger number (e.g., to three times as many records) would lower the estimated cost of not reissuing cards, since the effect of increasing this parameter would be to increase the estimation of the number of cards that are compromised, and thus lower the probability that any compromised card would be used for breach (since the extent of fraud would not change from this parameter). Because this number is unknown, we chose to use the broadest range as seems plausible.

The final factor in this calculation is the percentage of breached credit cards that are reissued before fraud occurs. To calculate the probability that an un-reissued breached card will be used for fraud, we estimate based on the number of un-reissued cards. A 2009 Maine study of bank responses to data breach incidents found that issuers reissued 78% of cards during the period covered by the survey, including 84% of accounts affected in the TJX breach and 77% of those affected in the Hannaford breach.[56] Based on this (admittedly non-representative) sample, the model uses the assumption that issuers re-issue between roughly 60% and 90% of cards, with a point estimate of 78%.

These data and assumptions lead to the estimated ranges listed in Table 5. Overall, we estimate that between about 2.5 million and 40 million unreissued credit card numbers are exposed in data breaches annually, with a point estimate of 12 million cards.

3.3.2 The Extent of Existing Credit Card Fraud

The best information on the extent of credit card fraud is compiled by the Department of Justice's Bureau of Justice Statistics (BJS), which reports per-household identity theft statistics as part of its annual National Crime Victimization Survey (NCVS).[57] These statistics are split out by the nature of the crime; "existing account credit card identity theft" refers to situations in which existing credit cards were used without the cardholder's

Table 5: Estimated total number of credit card records exposed in data breach per year (thousands)

Description	*Low*	*Point*	*High*
Payment card numbers reported lost in data breaches per year	35,000	38,000	41,000
Credit cards as percentage of breached payment cards	66%	72%	78%
Credit card numbers reported lost in breaches per year	23,100	27,400	32,000
Est. records per year in breaches with unknown record counts	150	2,900	7,500
Scaling factor to account for unreported or undetected breaches	1	1.34	2
Portion of breached cards reissued	0.90	0.78	0.60
Total estimated number of card records exposed in all breaches per year	2,460	12,000	40,600

[56] Me. Bureau of Fin. Inst., Maine Data Breach Study, Nov. 24, 2008, available at http://www.state.me.us/pfr/financialinstitutions/reports/index.htm

[57] *See* Lynn Langton, Bureau of Justice Stats., Pub. No. NCJ 236245, Identity Theft Reported by Households, 2005-2010 (2011) [hereinafter BJS 2011].

Table 6: Households in which at least one member was a victim of existing credit card fraud, 2005–2010, with standard errors (thousands)

	2005	2006	2007	2008	2009	2010
Households	2,971.9	3,623.7	3,894.3	--	4,986.5	4,625.1
Std. Err.	(130.4)	(145.1)	(143.6)		(174.1)	(152.7)

Source: Lynn Langton, Bureau of Justice Stats., Pub. No. NCJ 236245, Identity Theft Reported by Households, 2005-2010, at 7–8 (2011).

Note: The BJS collected only 6 months of data in 2008. Because of a change in methodology, caution should be used when comparing 2006 numbers to other years.

authorization.[58]

The survey statistics from the most recent NCVS report are listed in Table 6. For the most recent two years, about 4.6 to 5 million households were victims of at least one existing-account credit card fraud.

The BJS also published a special report in 2010 on identity theft victimization, based on supplemental questions added to the 2008 NCVS.[59] Unlike the annual NCVS surveys, the 2008 questions collected information about victimization per person rather than per household. Respondents were asked about their experiences with identity theft over the previous two years.

The 2010 survey found that about 4.8 million people had experienced at least one attempted or successful existing-account credit card fraud in the previous two years (with a standard deviation of 173,000).[60] This result is puzzling when compared to the annual survey data summarized in Table 6. The number of *households* that were victims of existing-account credit card fraud in *one* year should be lower than the number of *individuals* who were victims of attempted or successful existing-account credit card fraud over a *two* year period. But 4.8 million is about the same as the per-household annual figures in 2009 and 2010. And although it is larger than the 2007 and 2006 annual rates of 3,600 and 3,900 victimized households, it is not as much larger as one might expect given the conversion factor from individuals over two years to households over one year.

Comparing the credit card fraud data in Table 6 to the annual breach estimates in Table 2, as shown in Figure 5, is also instructive. Note that the incidence of existing-account credit card fraud is growing but stable, with no wild shifts from year to year. But the number of disclosed breached account numbers fluctuates wildly from year to year. What does that imply? A few explanations are possible. There could be large unreported breaches in the years with low breached record estimates. More plausibly, it could mean

[58] This type of "identity theft," which might more reasonably be termed unauthorized payment card use, stands in contrast to forms of "identity theft" that are more readily conjured by the term: "the misuse of personal information to open a new account or for another fraudulent purpose." BJS 2011, *supra* note 57, at 1.

[59] Langton & Planty, *supra* note 24.

[60] *Id.* at 11.

that megabreaches do not contribute to credit card fraud in proportion to their size, particularly if the market for stolen credit cards is stable (if growing). If that is the case, credit card megabreaches merely add to the supply of available stolen credit cards without drastically affecting the rate at which those cards are misused. This interpretation is consistent with reports that the market value of stolen credit card data has been depressed by oversupply.[61]

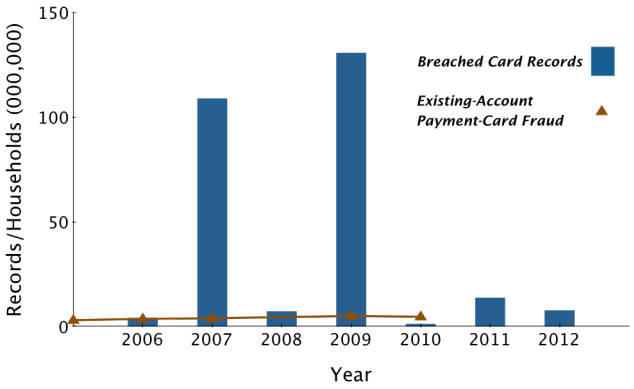

Figure 5: Annual breach estimates and credit card fraud

3.3.3 The Percentage of Existing Credit Card Fraud Attributable to Breach

Not all credit card fraud is the result of breach. Victims of existing-account credit card fraud who know how their card numbers were obtained most often say that it was through a stolen wallet or a purse or from someone they know. Breach seems to be a relatively infrequent cause of credit card fraud, but it is uncertain how infrequent.

Table 7 lists the responses in six surveys that asked if victims of identity theft knew how their information was obtained. In four of the six surveys, the most common answer was "I don't know." Of those who did knew how their information was obtained, between 6% and 17% identified a data breach as the point of compromise.

These numbers are subject to several caveats. First, most survey respondents did not know how their data was obtained. The responses of those who said that they knew how their data was obtained can be legitimately generalized only if the point of compromise and the victim's knowledge of that point of compromise are uncorrelated. But this may not be true. Some points of compromise are more likely to be known than others. Lost wallets, purses, or thefts alert a cardholder that their cards may have been stolen. Others, such as skimmers (devices that surreptitiously record card data at an ATM or point of payment) are unlikely to be recognized as a point of compromise. People whose cards are compromised through phishing or spyware will not always know that their cards were obtained in that matter. A data breach, of which a cardholder must be notified in forty-six of fifty states, may be more likely to be a known (or at least suspected) point of compromise.

[61] *See, e.g,* Brian Krebs, *I'll Take 2 MasterCards and a Visa, Please*, KREBS ON SECURITY, http://krebsonsecurity.com/2010/09/ill-take-2-mastercards-and-a-visa-please/ (Sept. 22, 2010, 2:21 AM).

Table 7: Responses to questions in six surveys asking if identity theft victims knew how their data was obtained, and, if so, the point of compromise

How Data Was Obtained	Javelin (2009)	Javelin (2006)	ITRC (2009)	FTC (2007)	CIMIP (2007)	BJS (2008)
Unknown	65%	54%	21%	56%	47%	64%
Known	35%	46%	79%	44%	53%	34%
Of those with a known point of compromise:						
Breach/company controlled	11%	6%	17%	11%	50%	11%
Transaction/scam/skimmer etc.	19%	22%	11%	16%		46%
Phish/hack/Internet	11%	8%	13%	5%	6%	10%
Lost/stolen from wallet, home, car, etc.	43%	30%	11%	11%	12%	24%
Knew thief	13%	15%	23%	36%	16%	3%
Stolen from mail	3%	8%	5%	5%	9%	2%
Other	1%	8%	15%	16%	8%	3%
Known breach/company controlled	4%	3%	13%	5%	26%	4%

Sources: Identity Theft Res. Ctr., Identity Theft: The Aftermath 2009, at 15 (2010), http://www.idtheftcenter.org/artman2/uploads/1/Aftermath_2009_20100520_1.pdf; Lynn Langton & Michael Planty, Bureau of Justice Stats., Pub. No. NCJ 231680, Victims of Identity Theft, 2008 (2010); Javelin Strategy & Research, 2009 Identity Fraud Survey Report: Consumer Version 7 (2009), http://www.idsafety.net/901.R_IdentityFraudSurveyConsumerReport.pdf; Gary R. Gordon et al., Ctr. for Identity Mgmt. and Info. Prot., Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement 53 (2007), http://www.utica.edu/academic/institutes/ecii/publications/ media/cimip_id_theft_study_oct_22_noon.pdf; Synovate, Federal Trade Commission—2006 Identity Theft Survey Report 5, 35 (2007); Javelin Strategy & Research, 2006 Identity Fraud Survey Report: Consumer Version 7 (2006).

Notes: Figures for the BJS study are for the point of compromise for existing-account credit card fraud only. All other sources report figures for all forms of identity theft. The CIMIP report did not distinguish between cases when a business was the point of compromise; thus, personal information obtained during a transaction is indistinguishable in that survey from data lost in a breach. "Known breach/company controlled" shows the number of respondents to the survey who believed that their data was obtained in a breach or from a company as percent of all responses including those cases in which the point of compromise was unknown.

A second caveat is that the survey with the highest percentage of known points of compromise and the highest percentage of people responding that their data was obtained in a breach is the ITRC survey. As the ITRC acknowledges, "[t]his may be due to the fact that ITRC is listed as a victim resource by many entities which have suffered a breach."[62]

Third, only the BJS survey reported responses for points of compromise specifically for existing-account credit card fraud. None of the other surveys distinguished between forms of identity theft in their reporting.

Finally, note that we tabulate data breach separately from compromise at the point of sale or during a transaction. These types of compromise are fundamentally different.

[62] Identity Theft Res. Ctr., Identity Theft: The Aftermath 2009, at 15 (2010), http://www.idtheftcenter.org/ artman2/uploads/1/Aftermath_2009_20100520_1.pdf.

Compromise during a transaction involves card data being stolen when the card is in use—for example, when a waiter writes down credit card numbers while charging the card, or when a skimmer records the card number at an ATM or card-swipe machine. If someone obtains more than nine cards in this manner, it is counted as a "breach" in the PRC database. But this type of "breach" is usually discovered after the fact when investigators notice a common thread between cards that have already been used fraudulently and canceled. This situation is irrelevant to an issuer's decision whether to reissue a credit card that has been exposed in a breach but not yet misused. Thus, these types of "breach" are excluded from this analysis. Note also that card skimming as a source of breach is essentially irrelevant to the total amount of breach (see Table 4).

Based on the factors listed above, we use a range of 5% to 15% as the proportion of existing-account credit card fraud in which the card information was obtained in a data breach, with a point estimate of 11% from the BJS report. We chose this range to capture, at the low end, either the lowest estimate for breach as a percentage of known points of compromise or the midrange of estimates for breach as a percentage of all compromise, including unknown sources. The high end of the range is just below the ITRC's number, which has a high number of people who believe they know how their information was obtained and the aforementioned potential bias toward identifying breach as the way credit card information was obtained.

Table 8: Financial loss from existing-account credit card identity theft by type of loss (for people who experienced at least 1 incident in the previous 2 years)

Loss Type	Mean Loss ($)	Std. Err.	Median Loss	% Exp. Loss	Std. Err.
Direct out-of-pocket	1,355	475	200	9%	1.0%
Indirect out-of-pocket	292	110	10	7%	0.8%
Total out-of-pocket	988	340	100	14%	1.1%
Total direct loss	1,105	87	400	59%	1.7%
Combined	1,086	91	400	61%	1.7%

Source: Lynn Langton & Michael Planty, Bureau of Justice Statistics, Pub. No. NCJ 231680, Victims of Identity Theft, 2008, at 14 (2010).

Notes: Direct loss includes "the value of goods, services, credit, loans, cash or anything else a person obtained while misusing personal information." Indirect loss "includes any additional costs incurred in the course of addressing the identity theft, such as legal fees, bounced check fees, and any miscellaneous expenses like postage, phone calls, or notary fees."

3.3.4 The Cost of Credit Card Fraud

The cost of an existing-account credit card fraud incident has two components: financial losses, including both the loss of value obtained through the fraud and indirect financial costs from responding to the fraud, and the cost of time spent dealing with the fraud.

In most cases, a cardholder should suffer little or no direct out-of-pocket costs from existing-account credit card fraud. Federal law limits cardholder liability to $50 for unauthorized credit card charges if a lost or stolen card is reported as soon as the loss or theft is discovered.[63] Visa and Mastercard have voluntary zero-liability policies that further reduce consumer liability for card fraud.[64] Despite these policies, cardholders may still experience out-of-pocket losses if they do not report lost or stolen cards quickly enough.

Table 8 lists the cost figures reported by the BJS 2010 survey. The survey found that the average combined direct and indirect loss was about $1100 for the 61% who experienced any loss. Table 10 lists the distribution of total value obtained in existing-account credit card frauds as reported in the 2006 Synovate/FTC report. Table 9 lists the distribution of the amount of time victims spent responding to these frauds. Based on these numbers, we estimate the range of average cost per existing-account credit card fraud at $1,000 to $1,500.

Table 9: Amount of time spent by victims of existing-account credit card fraud in resolving problems

Hours	*%*
≤ 1	45%
2–9	36%
10–39	12%
40+	8%
Median	2 hours
90th percentile	25 hours
95th percentile	60 hours

Source: Synovate, Federal Trade Commission—2006 Identity Theft Survey Report 5, 39 (2007).

Table 10: Distribution of the total value obtained by thief in existing-account credit card frauds

Value	*%*
< $100	20%
$100–$499	27%
$500–$999	14%
$1000–$5000	23%
≥ $5000	7%
Median	$350
90th percentile	$4,000
95th percentile	$7,000

Source: Synovate, Federal Trade Commission—2006 Identity Theft Survey Report 5, 35 (2007).

4 Analysis

Table 11 summarizes the basic analysis of the per-card cost of not reissuing cards, with ranges and point estimates.

[63] See 15 U.S.C. §§ 1643(a)(1)(B) (2006); 12 C.F.R. §§ 226.12(b) (2009).

[64] See Douglas Akers et al., *Overview of Recent Developments in the Credit Card Industry*, 17 No. 3 FDIC Banking Rev. 23, 32 n.46 (2005), available at http://www.fdic.gov/bank/analytical/banking/2005nov/article2.pdf

Table 11: Calculation of the expected cost per card of not reissuing cards

Description	*Low*	*Point*	*High*
Number of households victimized (1000s)	3,900	4,600	5,300
Percent of existing-account credit card fraud from breach	5%	11%	15%
Average number of credit cards per household[65]	6.25	7.88	9.50
P(existing-account credit card fraud | breach) ($\rho_{k,0}$)	0.0005	0.0056	0.0605
Mean financial cost of existing-account card fraud	$1,000	$1,366	$1,500
Hours spent responding to existing-account card fraud	1	8	15
Cost of time per hour[66]	$12	$15	$20
Cost of time spent responding to existing-account card fraud	$12	$130	$300
Total expected cost of and existing-account card fraud incident	$1,000	$1,500	$1,800
Fraud reduction from flagging exposed cards	0%	10%	20%
Expected cost per card of not reissuing cards	$0.41	$7.50	$109.00

Table 11 includes two parameters not already discussed: the number of credit card accounts per household and the fraud reduction from flagging exposed cards.

Converting from the per-household data reported by the BJS to per-account numbers requires an estimate of the number of credit cards per household. This seemingly simple statistic is actually difficult to quantify with precision. The 2012 Statistical Abstract of the United States reports a figure of 1.1 billion credit *cards* in 2009, which equates to 9.4 cards for each of the 117 million households in the U.S.[67] The original source for the Statistical Abstract data is the Nilson Report, an industry newsletter. Comparison of an issue of that newsletter from November 2008 with the Statistical Abstract shows that the Statistical Abstract indeed counts *cards*, not *accounts*.[68] The same Nilson report lists 1.04 billion accounts. The Federal Reserve Bank of New York's (FRBNY's) Consumer Quarterly Report on Household Debt and Credit also reports a number of credit cards accounts, but includes only accounts for bank-issued cards (thus excluding store cards, even if they carry Mastercard or Visa logos).[69] FRBNY reports a figure of about 380 million bank-issued

[65] *See* U.S. Census, Statistical Abstract of the United States t.59, t.1187, t.1188 (2012). For 2009, the abstract lists 1.1 billion credit cards excluding air travel plan cards, phone cards, auto rental, and miscellaneous cards. Dividing those 1.1 billion cards by 117 million households gives an estimate of 9.4 credit cards per household.

[66] Assumes an average annual wage of $45,500 per full-time employee, discounted 50% on the assumption that most time spent responding to breach occurs during non-work time. *See* U.S. Census, Statistical Abstract of the United States t.647 (2012).

[67] U.S. Census, Statistical Abstract of the United States t.59, t.1187, t.1188 (2012).

[68] *Compare* Nilson Report, November 15, 2008, at 10 *with* U.S. Census, 2010 Statistical Abstract of the United States, t.1151.

[69] E-mail from Donghoon Lee, Senior Economist, Federal Reserve Bank of New York, to Alessandro Acquisti, Professor of Information Technology and Public Policy, Carnegie Mellon University (Feb. 23, 2014, 10:38 AM EST).

Table 12: Comparison of the per-card cost of reissuing vs. not reissuing cards

Description	*Low*	*Point*	*High*
Reissue cost, per card	$3.00	$10.00	$25.00
Expected cost if not reissued, per card	$109.00	$7.50	$0.43
Per-card savings (cost) from not reissuing cards	($106.00)	$2.50	$25.00
Cumulative savings (cost) from not reissuing (mil.)	($3,400.00)	$68.00	$790.00

Note: Cumulative savings is based on the number of reported breach records, not the estimated total (see note 71).

credit card accounts for 2007.[70] This compares to 580 Mastercard, Visa, American Express, and Discover accounts reported in the 2008 Nilson report. Some of the discrepancy may be because the FRBNY panel data excludes inactive and canceled accounts that do not show up on credit reports. We use the Nilson report's figure for accounts as the maximum of our estimation range and scale the same number by the .65 ratio of the FRBNY's active-accounts bank card number to the FRBNY's bank-card number.. That results in a range of 6.25 to 9.5 credit card cards per household, with a point estimate of 7.875.

We assume that flagging exposed cards reduces fraud rates by up to 20%. As discussed in Section 3.3, current levels of fraud monitoring are already reflected in existing credit card fraud statistics. Thus, marking a card as potentially exposed can at best improve the effectiveness of fraud monitoring systems somewhat. Unfortunately, information on the effectiveness of fraud monitoring software is treated as proprietary by both issuers and the software vendors. The 0% to 20% range therefore represents our best guess.

Our model estimates the cost of not reissuing cards at between $0.41 and $109.00 per card, with a point estimate of $7.50. This wide range corresponds to a potential savings of $25 per card or loss of $106 per card. The point estimate is a $2.50 per-card savings by not reissuing. Taking total number of reported breached card numbers into account[71] implies that $68 million could be saved by not reissuing cards immediately after a breach. The range of estimation is extreme: $790 million might be saved, but the potential total loss calculated by this model is about $3.4 billion. Neither extreme is likely, however.

[70] Fed. Reserve Bank of N.Y., Quarterly Report on Household Debit and Credit 3 (Feb. 2014), *available at* http://www.newyorkfed.org/microeconomics/data.html. This figure includes only credit cards issued by banks, not store-issued cards.

[71] This number is used instead of the estimated total number of breached credit cards per year because issuers only face the reissue or do-not-reissue decision for cards they have reason to suspect were exposed in a breach. Issuers have no way to know which cards they might have to choose to reissue based on undetected and unreported breaches or breaches for which there is no estimate of the number of records exposed.

Table 13: Input variables and distributions used for Monte Carlo simulation

Variable	*Distribution*	*Range*
Per-card cost to issuer of reissuing cards	2+LogN(μ=8, σ=5)	[2,25]
Credit cards as a proportion of breached payment cards	N(0.72, 0.036)	
Card numbers reported lost in data breaches per year	N(38000, 2000)	
Est. records exposed per year in breaches with unknown record counts	N(2900, 1600)	
Scaling factor to account for unreported or undetected breaches	N(1.25, 0.275)	[1,∞)
Portion of breached cards reissued	N(.78, .09)	[0.5,1]
Number of households victimized (1000s)	N(4600, 350)	
Percent of existing-account credit card fraud from breach	N(.11, .075)	[.03,.20]
Average number of credit cards per household	N(7.875, 1.45)	
Mean financial cost of existing-account credit card fraud	Beta(α1=.25, α2=2.3, min=89, max=1300) [fitted]	
Hours spent responding to existing-account card fraud	.30+Γ(.235, 34.9) [fitted]	
Cost of time per hour	N(15, 2)	[12,20]
Fraud reduction from flagging exposed cards	N(0.1, 0.05)	

Note: All distributions were truncated to prevent negative values.

4.1.1 Monte Carlo Analysis

To get a better picture of the distribution along this wide range, we ran a Monte Carlo simulation. Table 13 lists the input variables used for the simulation and the distributions chosen. The distributions were chosen to reflect as closely as possible the ranges and assumptions already discussed. Each distribution was truncated to prevent negative values. We chose normal distributions for most variables, with means at point estimates and standard deviations that put our low and high estimates at about 5% and 95% probability in the distributions, respectively.

We model a few variables' distributions differently from this general approach. We model the per-card cost of reissuing cards as a log normal distribution with μ=8 and σ=5 because, as noted in section 3.2, we believe that the cost for most issuers is between $5–$10 per card, but with a long tail for a higher per-card cost in some cases. We truncated the scaling factor for unreported or undetected breaches at a lower bound of 1 (to prevent the scaling factor from reducing the total number of reported breaches) but set no upper limit on the distribution. This gave the parameter with a nominal μ=1.25 an actual mean of 1.34. The distributions for the mean financial cost of existing-account card fraud and the hours spent responding to existing-account card fraud were fitted to the distributions shown in Table 10 and Table 9, respectively.

We used a flattened normal distribution for the percent of existing-account credit card fraud that can be attributed to breach. Truncation at [.03, .20] creates a relatively

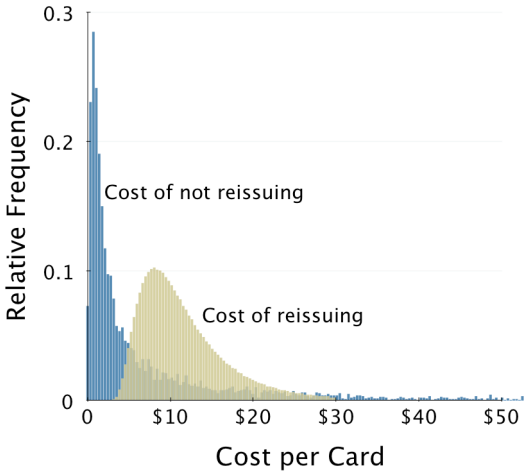

Figure 6: Distribution of the cost per card to reissue or not reissue cards based on a Monte Carlo simulation

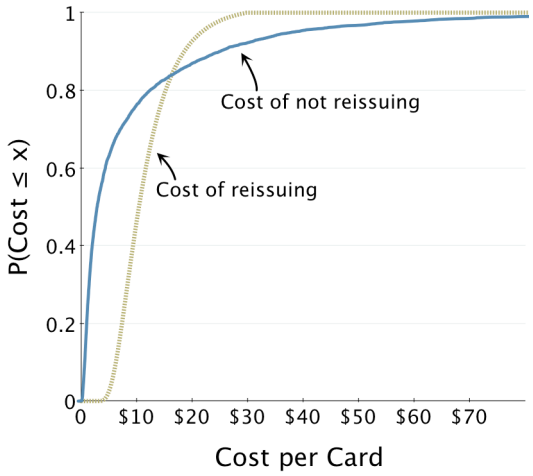

Figure 8: CDF comparison of the per-card cost of reissuing vs. not reissuing cards based on a Monte Carlo simulation

flat distribution; the 5%–95% range of the distribution falls within [.0414, .1870]. This choice reflects our lack of certainty in the proper value for this parameter.

The resulting distributions show a wide variation in possible costs, with some overlap between the reissue and no-reissue situations. Figure 6 shows a comparison of the histograms for each distribution. The bulk of the not-reissue distribution is at the low end, but with a long tail to the right. Figure 8 shows the CDF for each option.

Figure 7 shows a histogram of the total cost reduction that could be achieved from not automatically reissuing credit cards. The 90% confidence range is (–$790 million, $420 million), with a 26% probability that not reissuing costs more money than reissuing.

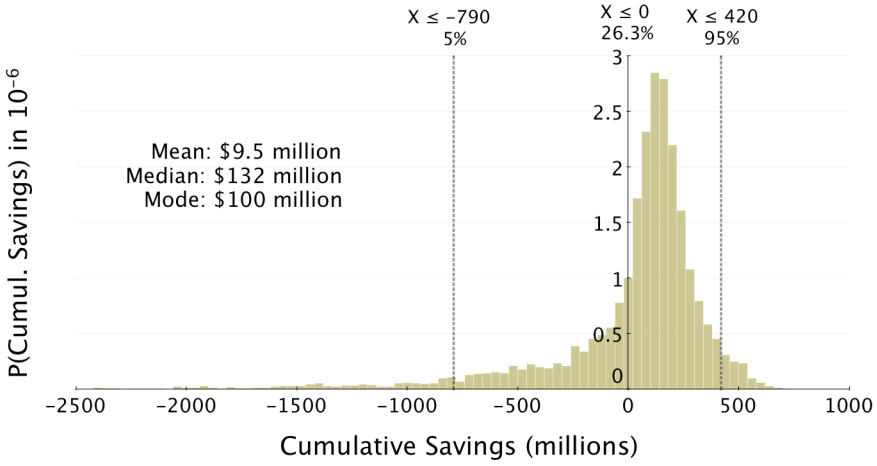

Figure 7: Histogram of cumulative savings from not automatically reissuing cards according to a Monte Carlo simulation

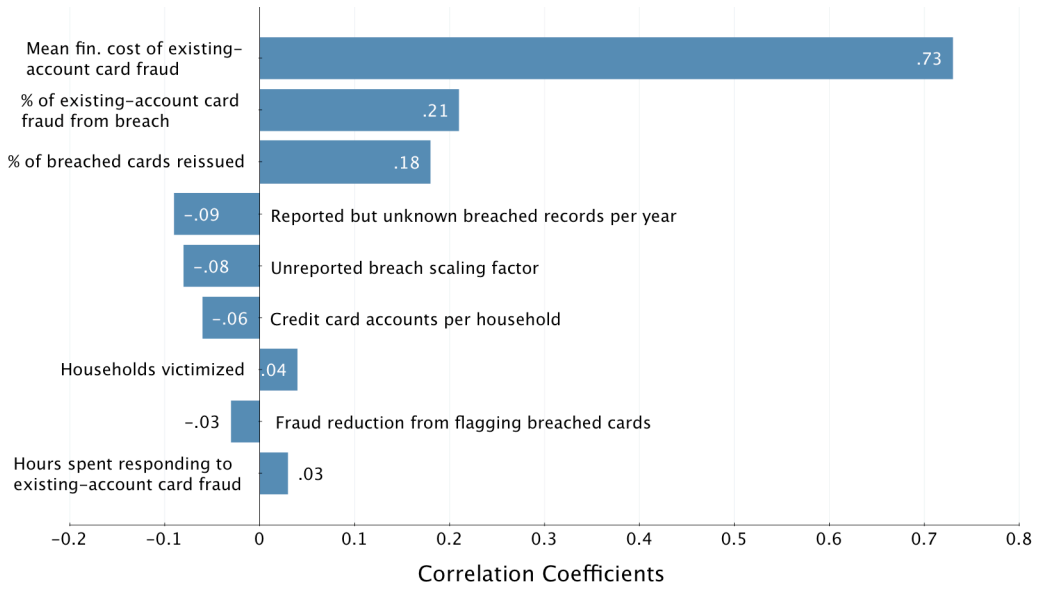

Figure 9: Tornado diagram of variables affecting the per-card cost of not reissuing cards

4.1.2 Sensitivity Analysis

Figure 9 is a tornado diagram showing the sensitivity of the per-card cost of not reissuing cards for the variables to which the cost is most sensitive. The cost of existing-account fraud is an important cost factor, as might be expected. The model is also sensitive to variables impacting the number of breached cards: the scaling factor for unreported breaches and the number of reported breaches with unknown record counts are both significant factors in the estimate, more so than is the number of records that are disclosed as breached each year (mostly because that number is better known).

The model is particularly sensitive to the percentage of existing-account credit card fraud attributable to breach. In fact the model is more sensitive to this parameter than any other except the cost of existing-account credit card fraud. This is also one of the least understood of the parameters. As we discussed in section 3.3.3, surveys are the most common source of data for how fraudulently used credit card information was obtained. In nearly all of the surveys we found on this subject, over half of respondents do not know how their information was obtained.

To further test the sensitivity of our model to this parameter, we first increased the simulation's upper bound limit of 0.20 on the parameter to 0.75 while leaving the standard deviation the same (the mean shifted up to 0.13 when the part of distribution above the former cutoff was added). The new upper bound is what we would get by assuming that data breach was responsible for all existing-account credit card fraud when no source was known. We ran a new Monte Carlo simulation with this new parameter. The distribution of total savings in this model has a 5%–95% range of $940 million in loss to $410 million in savings, with a mean of $21.5 million in loss and median of $125 million in savings. The

probability that not reissuing cards would result in a loss increases to 28.9% from 26.3% in the previous model.

We ran an additional simulation with the mean of this parameter increased to 0.20. We left the range capped at 0.75. The resulting probability of loss increased to 39.5%, with a mean loss of $180 million and median savings of $77 million. The 90% confidence range is $1.56 billion in losses to $360 million in savings.

The extent to which data breach is a cause of existing-account credit card fraud is clearly a critical parameter for the model. In fact, given the relative precision with which the financial cost of existing-account credit card fraud is known, the extent to which it is caused by breach is likely the most important unknown factor in determining whether the first order costs reissuing cards are more or less than the expected cost of fraud.

We also look at sensitivity to the scaling factor for the number of unreported or undiscovered breaches. Increasing the point estimate from μ=1.25 to μ=1.5 (which, with the cutoffs unchanged, increases the actual mean of the distribution from 1.34 to 1.52), the simulation gives a 90% interval of $680 million in loss to $420 million in total savings from not reissuing cards, with a mean savings of $48 million and median savings of $139 million. The probability of loss is 24.5%.

Reducing the estimated extent of undiscovered and undisclosed breach increases the estimated cost of not reissuing cards. If we set μ=1.15 and σ=0.5 (which puts the 90% interval for the distribution of this parameter at (1.07, 1.23)), the resulting 90% interval is $910 million loss to $40 million savings, with a mean of $15 million loss and median of $122 million saved. In this scenario, the probability that not reissuing cards would be a net cost is 29.3%.

4.1.3 Data quality issues

As the analysis of these two parameters shows, understanding the true costs of reissuing cards or not depends on estimating distributions of parameters when those distributions are not well known. Some of the unknowns are more unknown than others. Here, we briefly discuss this spectrum of unknowns and where the most important parameters in our model fit within this spectrum of unknowns.

There are several major types of unknowns, or data problems:

- The data does not exist and would be impossible or difficult to gather. The extent of undetected breach is an example of this type of unavailable data.
- Data exists but is not accessible. For example, we were unable to find estimates of how effective fraud monitoring software is in preventing credit card fraud. That information is likely well known by card issuers. The percentage of breached cards that are reissued is another parameter of this type: each issuer knows how many cards it reissues. When data quality issues of this type occur, the problem could be solved with greater cooperation from those who hold the data.

- Data exists but is of poor quality or varies across organizations. The data on data breach as a cause of existing-account credit card fraud is an example of this. Several surveys exist, but their results do not shed much light on the actual extent to which data breach is a cause of existing-account credit card fraud.

Our sensitivity analysis suggests that resources could be usefully targeted to getting better data for parameters critical to our model. Specifically, it would be useful to get better information on how identity thieves get access to credit card data. Surveys of victims are clearly not adequate; too many people simply do not know how their data was obtained. Issuers, however, have the ability to connect breach notification with card misuse. Issuers also have information, at least collectively, on the percentage of cards that they reissue after a breach. Access to this data would undoubtedly improve our understanding of the benefits of options following a data breach.

5 Second-Order Effects

The preceding analysis considers only first-order effects. We consider "first-order" effects to be the direct costs to cardholders, merchants, and issuers from reissuing cards or from fraud. For example, the first-order costs of reissuing to issuers include the costs of cutting and imprinting new cards, mailing them to cardholders, and handling customer-service requests related to the new cards. First-order costs to cardholders might include time spent validating receipt of new cards or updating their card numbers with merchants. Fraud losses represent first-order costs to whichever parties bear the loss.

But second-order effects are also important, especially considering the wide range in our estimation of the cost of not reissuing cards. We consider costs to be "second-order" if they may affect costs over time or are in some other sense a step removed from the immediate costs. Although we do not account for second-order effects in our model, here we briefly discuss these effects and their potential effects on our results.

5.1 Incentive Effects

Reissuing cards automatically after a breach may lower the market value of stolen credit cards, creating disincentives to attempts to steal credit cards or use stolen card data. If so, then not reissuing cards has a second-order cost: if issuers stopped reissuing credit cards after a breach, the value of a breach "haul" would increase because more of the records compromised in the breach would be valid. Cyberthieves would have more of an incentive to breach, which would increase the overall amount of credit card breach and therefore the total cost of breach.

That analysis assumes that the incidence of credit card theft through data breach is sensitive to the value of the stolen cards: the more stolen credit cards are worth, the more they will be stolen. But this may not be true. Research on underground carder markets may help with this question.

5.2 Increasing Fraud Window

The fact that many issuers automatically reissue cards could be a large reason why so little existing-account card fraud seems to result from breach—if most of the cards exposed in a breach are canceled as soon as the breach is discovered, there is a limited time window for the thieves to commit fraud. If issuers no longer reissued cards as a matter of course, the time window during which card fraud is possible would extend significantly (at least to the regular expiration date of the card). That would allow carders to "sit on" cards longer before using them, in turn making fraud detection harder.

An increasing window for fraud would also complicate efforts to trace the source of compromised card accounts. The more time between breach and misuse, the harder it is to connect the two, especially in the presence of intervening events (such as other data breaches).

5.3 Cardholder Expectations and Reduced Credit Card Use

Cardholder expectations are another important secondary factor. Cardholders may expect to have cards reissued automatically, and may feel less safe if cards are not reissued. But they also appear to be reluctant to use replacement cards after a breach.[72] Reduced usage of credit cards costs issuers money received in transaction fees and interest charges on account balances. The median credit card balance in 2007 was $3,000.[73] At an average 13.8% annual percentage rate, that reflects interest revenues of about $400 per card per year. Even a 10% reduction in a card's balance could cost $40 per year—more than any estimated replacement costs. Credit cards are also used for an average of $1500 in purchases per month.[74] At an average interchange fee rate of 1.5% to 2%, issuers receive between $22.50 and $30.00 in monthly interchange fees per card. A 10% reduction in spending translates to a $2.25 to $3.00 decrease in interchange fees. The income from these fees offsets related expenses, and thus the loss of the fees cannot be considered a direct "loss," but these numbers do suggest that when issuers decide whether to reissue cards immediately after a breach, the cost of lost activity on the card may be a significant factor.

[72] *See, e.g.*, Shirley W. Insco, Aite Group, Global Consumers React to Rising Fraud: Beware Back of Wallet 17 (2012). According to the report, "33% of consumers who received replacement cards [after a breach] state that they used the new card less frequently than the original card." But it is unclear whether this is because a card was reissued or because of the card exposure regardless of reissue. But cardholders may prefer fraud monitoring to cancelation. "Consumers are happiest when their financial institution detects fraud and brings it to their attention." *Id.* at 19.

[73] U.S. Census, Statistical Abstract of the United States t.1189.

[74] *Id.*, t.1188.

5.4 Summary

These second-order costs are potentially significant. The only second-order cost we have attempted to quantify—the cost of reduced credit card use—is alone enough to wipe out most of the expected (point estimate) cost savings from not reissuing cards.

6 Limitations, Assumptions, and Further Research

The results described in the previous section should be read with an understanding of the limitations involved. This section discusses some of those limitations.

The analysis described in this article treats breaches as homogeneous, assuming, for example, that a small number of records in an improperly discarded report creates the same risk of data exploitation as the hacking of a large database. This is almost certainly a poor assumption. It would be useful to attempt to model the effect of different forms of breach separately.

The model used in this analysis takes limited account of the wide variation in breach size. Nine known megabreaches (those potentially exposing one million or more unencrypted credit card or debit card records) account for 266 million of 277 million estimated records exposed from 2006 to 2012. Megabreaches may be quite different from most breaches. Excluding megabreaches requires more detailed information about them—particularly, the extent to which card data exposed in these megabreaches is used for fraud. An analysis that distinguishes megabreaches and "every day" breaches may find that the optimal strategy differs depending on the type of breach. For example, it may be that issuers should reissue cards after "everyday" breaches but not for megabreaches, or should reissue for hacking breaches but not for improperly discarded records.

The estimate for amount saved by not reissuing cards assumes that in the status quo, all cards exposed in breaches are reissued. To the extent that some issuers today do not reissue cards before detecting fraud, that would reduce the overall estimate of cost savings from not reissuing cards.

Finally, the obvious and major limitation (as well as motivation) of this work is the lack of data on the causes, extent, and effects of data breach. Efforts such as the National Cyber Leap Year[75] have attempted to fill this gap, but much more work is needed to create the type of data that can be used for reliable statistical analysis.

7 Conclusion

Based on our parameterized model, automatically reissuing cards after a breach seems to be more expensive than waiting for attempted fraud before reissuing. But this is only a first-order estimate, and one that has a wide range of uncertainty. That uncertainty

[75] Chong et al., National Cyber Leap Year Summit 2009, Co-Chairs' Report (2009), *available at https://www.qinetiq-na.com/wp-content/uploads/2011/12/National_Cyber_Leap_Year_Summit_2009_CoChairs_Report.pdf.*

is due partly to the fact that we rely on public data sources for our parameters and partly because the data sources themselves are subject to tremendous uncertainty. Furthermore, second-order costs may overwhelm our first-order results. Additional research, preferably with access to information held only by issuers, is needed to evaluate whether issuers should wait for attempted fraud before reissuing cards.