Measuring Identity Theft at Top Banks (Version 1.5)

Top Credit Card Issuers, Banks Ranked Under New Measures

March 31, 2008

By Chris Jay Hoofnagle[1]

[1] Senior Fellow, Berkeley Center for Law & Technology (BCLT), University of California-Berkeley Law.

The mission of the Berkeley Center for Law & Technology is to foster beneficial and ethical advancement of technology by promoting the understanding and guiding the development of intellectual property and related fields of law and policy as they intersect with business, science and technology. More information is available online at http://www.law.berkeley.edu/institutes/bclt/.

Introduction

This paper attempts to empower consumers, regulators, and businesses by providing information about the relative risk of identity theft[2] at major financial institutions. Many individuals commented on the first version of this paper,[3] including one who criticized the effort, using a comparison from the auto industry:

> *This is like grading Chevrolet on its corporate ability to avoid having its cars wreck. Sure, they'd prefer that their vehicles would never be involved in an accident, but since they aren't driving their cars (once sold) much less the other vehicles which may be involved in the accident, it's very tough for them to improve "their accident" statistics.*

This is an excellent comparison, but for different reasons than the commenter intended. Let me explain: Of course automobile manufacturers cannot control how people drive, but over the past 50 years, a market for auto safety has emerged, and the rate of traffic fatalities has decreased dramatically.[4] Understanding the factors that fostered an auto safety market, and a decrease in driving fatalities is worthwhile, because it illuminates the goals of *Measuring Identity Theft at Top Banks*. First, we must explore the commenter's metaphor in greater depth.

The commenter's metaphor expressed a frequent objection to the first version of this paper. Other commenters more explicitly stated that consumers are to blame for many identity theft incidents, because they fall for phishing attacks, they fail to secure personal information, or they allow family members or friends to steal their identity. But,

---

[2] "Identity theft" describes the use of another individual's personal information for fraudulent purposes. *E.g.*, Jennifer Lynch, *Identity Theft in Cyberspace: Crime Control Methods and Their Effectiveness in Combating Phishing Attacks*, 20 BERKELEY TECH. L.J. 259, 260 (2005). The most important distinction among types of identity theft are: "account takeover," where an impostor uses an established account, such as a credit card issued to a victim; and "new account fraud," where an impostor opens lines of credit in the victim's name. *See Identity Theft: How to Protect and Restore Your Good Name: Hearing Before the Subcomm. on Technology, Terrorism, and Gov't Information of the S. Comm. on the Judiciary*, 106th Cong. 33–34 (2000) (testimony of Beth Givens, Director, Privacy Rights Clearinghouse).

[3] *Measuring Identity Theft at Top Banks (Version 1.0)*, BERKELEY CENTER FOR LAW AND TECHNOLOGY, LAW AND TECHNOLOGY SCHOLARSHIP NO. 44, Feb. 26, 2008, *available at* http://repositories.cdlib.org/bclt/lts/44/.

[4] In 1966, the fatality rate per 100 million vehicle miles traveled was 5.5; in 2005, it was 1.45. U.S. DEPARTMENT OF TRANSPORTATION, TRAFFIC SAFETY FACTS 2005, available at http://www-nrd.nhtsa.dot.gov/pdf/nrd-30/NCSA/TSFAnn/TSF2005.pdf.

is blaming the consumer useful for solving problems? If this conversation begins and ends by slouching towards blaming the consumer for the problem, what opportunities will be missed?

Returning to the commenter's metaphor--if automobile safety were treated as an impossible challenge because of driver error, could progress be made in reducing traffic fatalities?

When automobile safety came to the attention of Congress and reformers in the 1960s, automakers highlighted the role of driver behavior and the relatively low rates of equipment failure in accident causation.[5] General Motors spent less than 1% of its budget relative to profits on safety.[6] Because drivers caused most accidents, automakers reasoned, driver education, rather than safety or design mandates, was the best solution to address harm.[7]

Today, driver error continues to cause most crashes, but it is understood in more nuanced ways, and technologies are being developed to help drivers avoid mistakes.[8] Empirical evidence drives technology adoption for accident avoidance,[9] and innovations ranging from the seat belt to the airbag help make accidents less harmful. The National Highway Traffic Safety Administration administers dozens of standards for crash avoidance and crashworthiness of cars,[10] and consumers can obtain crash safety and rollover information online.[11] Automakers such as Volvo have tied their brand name to

---

[5] Ralph Nader, UNSAFE AT ANY SPEED (Grossman 1965).

[6] *Id*. at 253-4.

[7] Chapters seven and eight of Ralph Nader's *Unsafe at Any Speed* discuss this debate in detail.

[8] RESEARCH AND INNOVATIVE TECHNOLOGY ADMINISTRATION, REDUCING MOTOR VEHICLE CRASHES WITH THE DOT'S INTELLIGENT VEHICLE INITIATIVE, May-June 2002, available at http://www.volpe.dot.gov/infosrc/highlts/02/mayjune/d_focus.html.

[9] Laura Meckler, *New Car-Safety Focus: Crash Prevention --- Regulators to Propose That All Vehicles Include Stability Control; Weighing Warning Systems*, WALL STREET JOURNAL, Sept. 14, 2006.

[10] NATIONAL HIGHWAY TRANSPORTATION SAFETY ADMINISTRATION, SAFETY ASSURANCE, n.d., *available at* http://www.nhtsa.dot.gov/cars/rules/import/FMVSS/index.html

[11] *See* http://www.safercar.gov.

vehicle safety,[12] and sophisticated safety equipment is available even in less expensive cars.[13] This is all evidence of a vigorous market for automobile safety, a market that could have not developed if the debate did not transcend the driver error problem.

Many parallels exist between automobile safety, and, for lack of a better term, bank safety—the prevention of a panoply of fraud-related harms, such as identity theft and phishing. Just as consumers lacked safety information on cars in the 1960s, today we lack reliable methods to understand risk of identity theft at banks. Without such tools, a market for bank safety cannot emerge; institutions cannot "race to the top" to shield consumers from fraud.

In earlier work, I have argued that to address these problems, lending institutions should publicly report basic statistical information about identity theft events.[14] In the UK, a basic fraud statistics-reporting network already exists.[15] We could improve upon that system by reporting the number of identity theft events suffered or avoided; the form of identity theft attempted and the product targeted (e.g., mortgage loan or credit card); and the amount of loss suffered or avoided. With reporting, consumers, regulators, and businesses could more accurately assess the identity theft problem and respond appropriately.

Since identity theft reporting is not on the legislative horizon in the US, this effort seeks to find proxies for reporting by banks. Thus, the Freedom of Information Act was used to obtain complaint data submitted by victims in 2006 to the Federal Trade Commission (FTC). This complaint data identifies the institution where impostors established fraudulent accounts or affected existing accounts in the name of the victim. The data were then aggregated and used to rank institutions. The methods section

---

[12] Volvo operates a "The Volvo Saved My Life Club" online. *See* http://www.volvocars.com/us/footer/about/VolvoSavedMyLifeClub/Pages/default.aspx.

[13] Jonathan Welsh, *Cheaper Cars Move to Top Of Safety List --- Insurers Give Highest Rating To 9 Vehicles Under $30,000; Kia and Hyundai Join Mercedes*, WALL STREET JOURNAL, Nov. 21, 2006.

[14] *See Identity Theft: Making the Known Unknowns Known*, 21 Harv. J. L. Tech. 97 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/HOOFNAGLE_Identity_Theft.pdf.

[15] CIFAS, 2007 FRAUD TRENDS, n.d., *available at* http://www.cifas.org.uk/default.asp?edit_id=790-57.

explains in detail the imperfections of this approach, and commenters have suggested new techniques and challenges to be overcome.

The author continues to welcome constructive criticism, suggestions, and comments in an effort to create a more perfect picture of identity theft. The most effective and obvious improvement on this effort would come from voluntary reporting of fraud statistics by institutions themselves.

Methods and Challenges in Measuring Identity Theft

This analysis suffers from several methodological challenges, but progress on many of these challenges was made in version 1.5, thanks to the contribution of several commenters. The sections below explain ongoing challenges with the FTC data that identifies institutions, the Federal Deposit Insurance Corporation (FDIC) and other data that is used to compare the size of institutions, and other, general challenges.

The Federal Trade Commission Consumer Complaint Data

The FTC collects information from identity theft victims by phone and through an online form.[16] In doing so, the FTC requests that victims: "Please identify companies or organizations where fraudulent accounts were established or your current accounts were affected…" In the form used to process this data, victims are asked to identify up to three companies where accounts were established or affected. While the FTC performs an annual analysis of this complaint data, the agency does not publicize the names of institutions identified by victims.[17] The Freedom of Information Act (FOIA) was used to request this data, along with additional, non-personally identifiable information provided by victims.

The request, sent May 16, 2007, resulted in negotiation with the FTC on the scope and amount of records requested. The original request sought two years of data, but in light of the burden upon the FTC's disclosure office to review and release hundreds of

---

[16] *See* FEDERAL TRADE COMMISSION, COMPLAINT INPUT FORM, *available at* https://rn.ftc.gov/pls/dod/widtpubl$.startup?Z_ORG_CODE=PU03.

[17] *See* FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2007 (Feb. 2008), *available at* http://www.ftc.gov/opa/2008/02/fraud.pdf.

thousands of complaints (the FTC received 674,354 complaints in 2006; 246,035 were identity theft related[18]), the request was limited to three randomly-chosen months in 2006, January, March, and September. These months included data from 88,560 complaints, with 46,262 names of institutions were identified by victims.

The first disclosure covered data collected in January 2006 (FTC reference numbers 7384481 to 7773871); the second disclosure covered March (7752733 to 7943922) and September 2006 (8926143 to 9093712), in two separate files. Both disclosures were made in February 2008. Table 1 compares these disclosures.

Table 1: FTC Complaint Data Obtained Under FOIA

Date Complaint Submitted by Victim	Reference Numbers of Complaints	Total Number of Complaints Obtained	Number of "Institution" Rows with Text	Institution Rows After Disqualifying Blanks and Unknowns
January 2006	7384481 to 7773871	29945	19002	16582
March 2006	7752733 to 7943922	33161	20011	16168
September 2006	8926143 to 9093712	25454	16090	13512
Totals		88560	55103	46262

All the responses from the three company fields were concatenated, and blank rows, extraneous data (obvious errors, such as zip codes), and rows containing content such as "unknown" or "not provided" were eliminated. The data were adjusted where inconsistent or misspelled names were used (e.g., Wallmart, Citybank, Bank of American), combined where companies that, as of 2006, were merged but nevertheless

[18] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2006 (Feb. 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

were identified as separate companies by consumers (e.g., AT&T Wireless and Cingular, JP Morgan and Chase), and consolidated when corporate names were merged with a specific product (e.g., "Citibank Visa" became "Citibank").

Institutions were then ranked in order from high to low by number of fraud events. This means that the number of fraud events is counted differently than complaints. In fact, it is common for a single identity theft complaint to describe several events of fraud, and several institutions involved in the fraud. Therefore, for purposes of this analysis, any mention of a company name (each complaint allows victims to enter up to three) is an event that was counted for purpose of calculating the overall number and relative rate of identity theft.

This analysis could benefit from the inclusion of more data, especially data indicating whether the events submitted by victims pertained to account takeovers or new account fraud. A variety of consumer protection laws and self-regulatory practices limit liability for financial account takeovers.[19] However, regulations and self-regulatory practices associated with credit cards are more advantageous to consumers than protections associated with debit/ATM cards. Therefore, an account takeover of a credit card may have less financial impact to a consumer than the takeover of a debit/ATM card. When a non-credit account, such as a checking or savings account, is hijacked, the victim can be left with no money and no ability to pay bills. Despite regulatory protections for consumers' accounts, in many cases, consumers do not recover the full amount of the fraudulent charges. In 2004, according to Gartner, consumers recovered 80% of losses from Phishing attacks. In 2005, only 54% recovered the full amount of fraud.[20] Accordingly, information distinguishing between account takeovers and new account frauds would be instructive, because account takeovers present a different type of risk and harm than new account fraud, and these two types of the fraud can be addressed in different ways.

---

[19] See e.g. Regulation Z, 12 C.F.R. § 226; Regulation E, 12 C.F.R. § 205.

[20] Robert McMillan, *Consumers to Lose $2.8 Billion to Phishers in 2006, Experts say phishing attacks continue to rise, getting more costly*, PC World, Nov. 9, 2006, available at http://www.pcworld.com/article/id,127799/article.html.

This analysis is based upon complaints submitted by consumers to the FTC. The FTC has found that "Most victims of ID Theft do not report the crime to criminal authorities."[21] This may especially be the case with account takeovers, because many victims resolve the issue with a call to the institution without further inconvenience.[22] "Synthetic identity theft" events, defined by the FTC as, "Situations in which someone creates a fictitious identity by combining personal information from one or more consumers with invented information, rather than using the identity of an existing individual,"[23] may not be reflected by consumer complaints. As a result, this analysis undercounts the total number of identity theft events in the months analyzed.

Several factors complicate victims' identification of institutions. The FTC's identity theft complaint form is lengthy and takes substantial time to complete. Victims identify institutions near the end of the form, when they may be fatigued or hurried to complete the task of submitting the complaint. The FDIC alone regulates over 8,600 banks; some have similar names or use neologisms that are difficult for individuals to spell. Banks may use the same name to represent different legal entities. These factors, combined contribute to ambiguity in the names of some institutions. For instance, a victim submitting "AT&T" might intend to mean AT&T wireless, long distance service, internet service, or even an AT&T-branded credit card. Similarly, when a victim enters "Citibank," there often is no way to determine whether the victim intends "Citibank National Association" or "Citibank (South Dakota) National Association."

Similar ambiguities are present when a victim identifies a retailer, such as Target as the institution involved in the fraud. The victim could mean that Target issued a credit card in the victim's name, that the victim's Target credit card was used fraudulently, that a

---

[21] FEDERAL TRADE COMMISSION, IDENTITY THEFT SURVEY REPORT 9 (Sept. 2003), available at http://www.ftc.gov/os/2003/09/synovatereport.pdf.

[22] 38% of credit card fraud victims reported "no problem" or that they resolved the incident within one day. FEDERAL TRADE COMMISSION – IDENTITY THEFT SURVEY REPORT 25 (Nov. 2007), *available at* www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

[23] FEDERAL TRADE COMMISSION – IDENTITY THEFT SURVEY REPORT (Nov. 2007), *available at* www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

different credit card was used for fraudulent charges at Target, or that their account on Target.com was phished.

Betsy Broder, the Assistant Director of the Federal Trade Commission's Division of Privacy and Identity Protection, commenting on version 1.0, provided important considerations with respect to the consumer complaint data. Broder amplified the above-mention concerns: "complaint data may contain errors and may not correctly identify the company that is associated with the identity theft."[24] Broder concluded that this and other limits of the FTC data fundamentally weaken the analysis:

> *I am concerned that some readers of the report and, more likely, readers of the press accounts about it, will ignore the caveats in your report and place great weight on its findings than is warranted. In addition to the questions about the underlying data as described above, we believe it would be erroneous to extrapolate from the complaints that the companies with the highest number of complaints were either greater sources of data breaches or had especially lax procedures for opening new accounts.*[25]

Broder's objection is a serious one, but version 1.0 carefully set forth weaknesses in methods, with a goal of improving upon them. Version 1.5 improves upon them substantially, with better measures of institution size. Neither this version nor the first makes conclusions concerning security breaches or the particular problem of new account fraud. The relationship between security breaches and identity theft cannot be determined with the numbers available in this analysis. Furthermore, the data available do not separate new account and account takeover frauds, accordingly, new account procedures cannot be assessed.

This is an iterative process, one that will require continual tuning. Much like the appreciation for the complexity of auto safety has progressed over time, our understanding of identity theft risk is likely to evolve as well. The fact that some will

---

[24] Letter from Betsy Broder, Assistant Director, Division of Privacy and Identity Protection, FTC, to Chris Hoofnagle, Senior Fellow, Berkeley Center for Law & Technology (Mar. 6. 2008), *available at* https://webfiles.berkeley.edu/choofnagle/public_html/Chris%20Hoofnagle%20Letter.pdf.

[25] *Id*.

(and have) misinterpreted the message of the report is not a compelling reason for ending this inquiry.

Broder suggested a second weakness in using the FTC data to rank institutions: "some companies take special efforts to direct consumers to the FTC's complaint system," accordingly, these institutions "may have a disproportionate number of complaints" in the database.[26] The FTC receives complaint data from the Better Business Bureau and the Identity Theft Assistance Center (ITAC), the later of which has submitted more than 29,000 complaints to the FTC database.[27]

ITAC was created in 2004 by the "Financial Services Roundtable and BITS, which represent 100 of the largest integrated financial services companies."[28] ITAC's membership page includes 16 of the top 25 banks that are the focus of this paper.[29]

The FTC receives about 250,000 complaints of identity theft annually,[30] making ITAC's 29,000 contribution a small percentage of the overall number of complaints. Furthermore, the fact that so many top banks are members of ITAC, Better Business Bureau, or the Financial Services Roundtable suggests that these organizations' recommendations to victims may be distributed fairly. Still, Broder's comment is a strong one, because several large banks, including JP Morgan Chase and Washington Mutual, are not listed as members of ITAC. These entities may have a higher rate of fraud that this report suggests.

Despite these institutions' lack of participation in ITAC, both JP Morgan Chase and Washington Mutual perform poorly on almost every measure in version 1.5, even

---

[26] *Id*.

[27] *Id*.

[28] IDENTITY THEFT ASSISTANCE CENTER, WHAT IS THE IDENTITY THEFT ASSISTANCE CENTER?, n.d., *available at* http://www.identitytheftassistance.org/questions.html.

[29] IDENTITY THEFT ASSISTANCE CENTER, ABOUT ITAC, *available at* http://www.identitytheftassistance.org/members.html

[30] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2007 (Feb. 2008), *available at* http://www.ftc.gov/opa/2008/02/fraud.pdf.

relative to larger institutions that do participate in ITAC. This lack of participation combined with relatively high rates of fraud suggests that ITAC members have not been heavily overrepresented by virtue of their participation.

A Bank of America spokesperson remarked that institutions named in a consumer complaint may not have caused the fraud:

> *Bank of America spokeswoman Betty Riess says the company hasn't seen the study yet, but says BoA takes security seriously. "Keep in mind that if we have a customer who reports they are a victim of identity theft that doesn't correlate to security at BoA," Riess said, referring to the fact that a BoA customer experiencing identity theft could have had their mail stolen or fallen prey to a phishing attack. "Protecting customer information is a top priority at BoA and we have multiple layers of security." Riess added that BoA uses online security offerings from RSA and lets customers use one-time credit card numbers for purchases from unfamiliar online retailers.*[31]

Riess and others[32] often invoked phishing as an example of a situation where the consumer's mistake resulted in identity theft. As noted in the introduction, some of the most strenuous objections to version 1.0 came from bank security officers frustrated with individuals' inability to recognize phishing attacks. This objection to the analysis is myopic. While phishing has imposed substantial costs on online banking, other types of attacks dominate the FTC complaint data. The FTC's analysis of the identity theft complaint data shows that victims suffered a variety of identity-related frauds, a high percentage of which were attacks that established new accounts.[33]

---

[31] Ryan Singel, *Bank of America, HSBC Most Prone to I.D. Theft, Report Says – Updated*, Threat Level, Feb. 27, 2008, available at http://blog.wired.com/27bstroke6/2008/02/bank-of-america.html.

[32] *See e.g.* "Harry Calamari" commenting that "nearly all information breaches are most often due to the negligence of the consumer," on *More Accurate Identity Theft Reporting By Banks: The Opening Salvo*, Bank Lawyer's Blog, Mar. 9, 2008, *available at* http://www.banklawyersblog.com/3_bank_lawyers/2008/03/more-accurate-i.html.

[33] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2006, 13 (Feb. 2007), *available at* http://www.consumer.gov/sentinel/pubs/Top10Fraud2006.pdf.

Further, as explained in the introduction, one of the assumptions of this effort is that fraud events can be shaped by institutions' policies,[34] and some events are clearly the fault of the institution.[35] As Riess noted, mail theft is outside the bank's control, but one of the principal reasons mail is stolen is to intercept bank-initiative marketing communications, such as pre-approved credit offers. Almost 8 billion of these solicitations are sent annually,[36] each offering a chance for impostors to open new accounts.[37] Adding to this is an enduring problem in credit granting—that the Fair Credit Reporting Act's standard for access to credit reports (which enables businesses to grant

---

[34] In a December 2007 workshop on Social Security Numbers held by the Federal Trade Commission, Trey French of Bank of America stated that the bank approved about 14 million credit applications a year mostly through a completely automated process, meaning that the institution had no human review of this account granting. An institution that decides to do such a thing will have a different identity theft footprint than other banks. Tramond French, Vice President, Bank of America, Remarks at Security in Numbers, SSNs and ID Theft, Federal Trade Commission Workshop (Dec. 10, 2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/index.shtml.

[35] See, e.g., *Wolfe v. MBNA Am. Bank*, 485 F. Supp. 2d 874 (W.D. Tenn. 2007) (permitting negligence claim against defendant bank to continue under Tennessee law where a fraudulent credit application was accepted despite having a false address, phone number, and mother's maiden name); My earlier paper, *Identity Theft: Making the Unknown Knowns Known* shows that it is possible to manufacture "synthetic" identities using real Social Security numbers (SSNs) and fake names in order to obtain credit, suggesting that some institutions do not even match SSNs to the applicant's name. 21 Harv. J. L. Tech. 97 (2007), available at http://jolt.law.harvard.edu/articles/pdf/v21/HOOFNAGLE_Identity_Theft.pdf. A recent draft FDIC report obtained by Brian Krebs of the Washington Post describes a synthetic fraud scheme causing $14 million in losses. FEDERAL DEPOSIT INSURANCE CORPORATION, TECHNOLOGY INCIDENT REPORT (Nov. 9, 2007), available at http://blog.washingtonpost.com/securityfix/2008/03/the_fdic_computer_intrusion_re.html.

[36] Julia Spencer, *Card Mail*, Cardtrak.com, Feb. 21, 2007, *available at* http://www.cardtrak.com/news/2007/02/21/card_mail.

[37] See, e.g., Bob Sullivan, *Even torn-up credit card applications aren't safe*, MSNBC, Mar. 14, 2006, available at http://redtape.msnbc.com/2006/03/what_if_a_despe.html; *Identity thieves feed on credit firms' lax practices*, USA TODAY, Sept. 12, 2003, p. 11A; Kevin Hoffman, *Lerner's Legacy: MBNA's customers wouldn't write such flattering obituaries*, CLEVELAND SCENE, Dec. 18, 2002; Scott Barancik, *A Week in Bankruptcy Court*, ST. PETERSBURG TIMES, Mar. 18, 2002, p 8E. The lax standards associated with new account opening with prescreened offers are illustrated by cases where accounts have been opened in the name of dogs. *See e.g. Dog Gets Carded*, Wash. Times (Jan. 30, 2004), available at http://washingtontimes.com/upi-breaking/20040129-031535-6234r.htm; *Dog Issued Credit Card, Owner Sends In Pre-Approved Application As Joke*, NBC San Diego (Jan. 28, 2004), available at http://www.nbcsandiego.com/money/2800173/detail.html.

new credit accounts) is so low that individuals have no effective way of avoiding identity theft, short of employing a credit freeze.[38]

Since there are so many banks in the US, and because they operate under different names, there is a risk that some institutions will not be associated with all of their affiliates. This can cause larger banks to have a lower incidence of fraud.

This report relies upon 2006 data, the most recent available, because of the delay associated with requesting information under the Freedom of Information Act.[39] The data were requested in May 2007, but not received until February 2008. This delay may cause the analysis to not fully reflect risk to customers in 2008, because of trends in identity theft. An analysis for 2007 will be performed as soon as data are available.

Jesper Johansson suggested that future analyses should include larger, more representative data sets.[40] Johansson's suggestion is based in part on the idea that fraud rates wax and wane over the year, and certain months reflect more fraud than others. Indeed, the three months analyzed here reflect periods with high numbers of consumer complaints--88,560 of the 246,035 received by the FTC in 2006. The 2007 data again will use a three month sample, but different months were randomly selected for that future report.

Data Used to Compare Institutions

In version 1.0, institutions were ranked by size according to their total deposits in December 2006, according to the FDIC's SDI database.[41] Total deposits includes: "The

---

[38] *Putting Identity Theft on Ice: Freezing Credit Reports to Prevent Lending to Impostors*, in SECURING PRIVACY IN THE INTERNET AGE, Stanford University Press, forthcoming 2008, *available at* http://ssrn.com/abstract=650162.

[39] This delay formed the basis of some individuals' criticisms: Commenting on Threat Level, "paual" wrote, "…What is really frustrating about this study is the fact that the data is up to two years old. What has changed since that time? Are these companies any more secure?" Ryan Singel, *Bank of America, HSBC Most Prone to I.D. Theft, Report Says – Updated*, Threat Level, Feb. 27, 2008, available at http://blog.wired.com/27bstroke6/2008/02/bank-of-america.html.

[40] Jesper Johansson, *Measuring Identity Theft*, Feb. 29, 2008, *available at* http://msinfluentials.com/blogs/jesper/archive/2008/02/29/measuring-identity-theft.aspx.

[41] Available at http://www2.fdic.gov/sdi/index.asp.

sum of all deposits including demand deposits, money market deposits, other savings deposits, time deposits and deposits in foreign offices." Rate of fraud was calculated by estimating the annual number of fraud events (based on three months of data) and dividing the estimate by the institutions' deposits, in billions of dollars.

Several commenters amplified weaknesses identified in version 1.0 concerning use of the total deposit figure, and others identified additional problems. An unidentified HSBC bank official was quoted by the San Francisco Chronicle as stating that use of total deposits unfairly portrayed the institution, because the bank has a large non-depository customer base:

> *"In our initial review of the study, we believe it is not accurate," the bank said. "To be valid, the study should have used as a measure our total U.S. customer base when instead it erroneously used our bank deposit base, which represents only 16 percent of our customers in the United States."*[42]

Commenting on the same article, "nezumi" levied a different criticism—that using total deposits make banks appear to perform better because large, corporate accounts were counted in the measure:

> *The statistics presented are meaningless. ID Theft by number of active consumer accounts (not commercial accounts) would provide a more accurate picture. $ Deposits can dilute the impact of institutional investing in overnights, time deposits, and CDs to make the situation look better than it actually is.*[43]

Soliciting comment on version 1.0 was helpful, because commenters not only identified weaknesses in the methods, but also suggested solutions. "jm," commenting on Threat Level, wrote:

> *A better analysis [would] break out the cases of identity theft based on the type of account (checking, savings, debit card, credit card,*

---

[42] Deborah Gage, *Banks, phone companies identity-theft targets*, San Francisco Chronicle (Feb. 27, 2008), available at http://www.sfgate.com/flat/archive/2008/02/27/chronicle/archive/2008/02/27/BUC7V9OV6.html?tsp=1.

[43] Deborah Gage, *Banks, phone companies identity-theft targets*, San Francisco Chronicle (Feb. 27, 2008), available at http://www.sfgate.com/flat/archive/2008/02/27/chronicle/archive/2008/02/27/BUC7V9OV6.html?tsp=1.

etc.) involved and report incidents per customers of that account type. That would give a clearer picture of what's going on.[44]

Version 1.5 improves on these methods substantially by including several new measures of institution size, many of which were identified by commenters.

First, the Nilson Report offers a ranking of credit card issuers by volume of cash advances and purchases made. Nilson Report data from 2006 is used to rate the top 10 credit card issuers by volume. This measure should more fairly portray institutions such as HSBC and other major credit card issuers that have a small depository account footprint.

The Nilson Report's data is proprietary and its sources are not always clearly stated. The publication claims to be, "the world's leading source of news and proprietary research on consumer payment systems."[45]

Second, Paul Witman, a professor with California Lutheran University's School of Business, made suggestions for improving the FDIC data used in version 1.0. He suggested using "Number of deposit accounts of $ 100,000 or less," a FDIC statistic that is only offered in reports submitted in June. It is defined as, "Number of deposit accounts of $100,000 or less held in domestic offices."

Third, two additional FDIC measures are incorporated in version 1.5. "Deposit accounts of $100,000 or less," and "Retail deposits" should help focus in on consumer-controlled accounts, and exclude larger, corporate accounts. Deposit accounts of $100,000 or less is defined as "Amount of deposit accounts of $100,000 or less held in domestic offices and in insured branches in Puerto Rico and U.S. territories and possessions." Retail deposits is defined as, "Total domestic office deposits minus time deposits of $100,000 or more held in domestic offices."

---

[44] Ryan Singel, *Bank of America, HSBC Most Prone to I.D. Theft, Report Says – Updated*, Threat Level, Feb. 27, 2008, available at http://blog.wired.com/27bstroke6/2008/02/bank-of-america.html.

[45] *See* http://nilsonreport.com/.

These new FDIC measures should be useful in comparing banks with strong consumer deposit bases, but institutions with large credit card operations will fare worse under this measure.

Other Methods Challenges

In addition to the challenges presented by the FTC, FDIC and Nilson data, several other problems remain unresolved:

Telecommunications companies ranked highly in overall events, but their relative rates of fraud are not compared here. Jesper Johansson suggested several sources for obtaining data on wireless subscribers, most of which are self-reported by telecommunications companies. I prefer to use statistics reported to a government entity where possible, but will incorporate self-reported or proprietary data if officially reported statistics are not available. As a result, no analysis of relative incidence is performed between carriers and banks, or among carriers themselves in this version.

Jesper Johansson provided an in-depth critique of version 1.0, with many helpful suggestions for new metrics to understand the identity theft problem:

> *Why is it that some institutions have a far greater incidence of identity theft than others? At this point, I think we need some hypotheses about the contributing factors, including customer demographics, number of customers, size of the accounts, the ease with which account takeover can be monetized, the protective measures in place at the institutions, the type of advice given to customers, and so on. This requires far more data gathering, and some multivariate analysis of the impact of each variable on the number of accounts stolen.*[46]

These are excellent suggestions. The types of marketing solicitations (e.g. prescreened offers of credit and convenience checks) would also be helpful in focusing on identity theft rates. As data on these factors become available, they will be incorporated in future versions of this analysis.

---

[46] Jesper Johansson, *Measuring Identity Theft*, Feb. 29, 2008, *available at* http://msinfluentials.com/blogs/jesper/archive/2008/02/29/measuring-identity-theft.aspx.

Final, several commenters remarked that version 1.0 simply stated the obvious: larger banks were bigger targets of scammers, and thus one should expect larger institutions to fare worse on identity theft. This statement was perhaps best expressed by Patrik Jonsson, who reported that "…many banks say the Hoofnagle study simply told people what they already knew -- that the biggest banks are going to have the most problems with fraud."[47]

This assumption that larger banks have bigger fraud problems is not obvious, and probably contradicts many consumers' expectations. It would be perfectly rational for a consumer to assume that a big, reputable bank would have more sophisticated systems and more intense investment in security systems than a smaller bank or credit union, and thus conclude that larger institutions are harder to attack. This assumption also contradicts some of the promises underlying the recent laws that allow permissive information sharing among bank affiliates. Proponents of information sharing argued that more opportunities to share personal information would help in identifying and fighting fraud.[48] Combined, these factors may lead individuals to believe that bigger banks are safer.

Taken together, these limits point to the need for identity theft reporting by institutions themselves, as outlined in *Identity Theft: Making the Unknown Knowns Known.*[49] A more complete picture of identity theft will not emerge until institutions provide more transparency on the problem.

---

[47] Patrik Jonsson, *New Identity Theft Study Meets Mixed Reviews*, Bank Info Security, Mar. 17, 2008, *available at* http://www.bankinfosecurity.com/p_print.php?t=a&id=755.

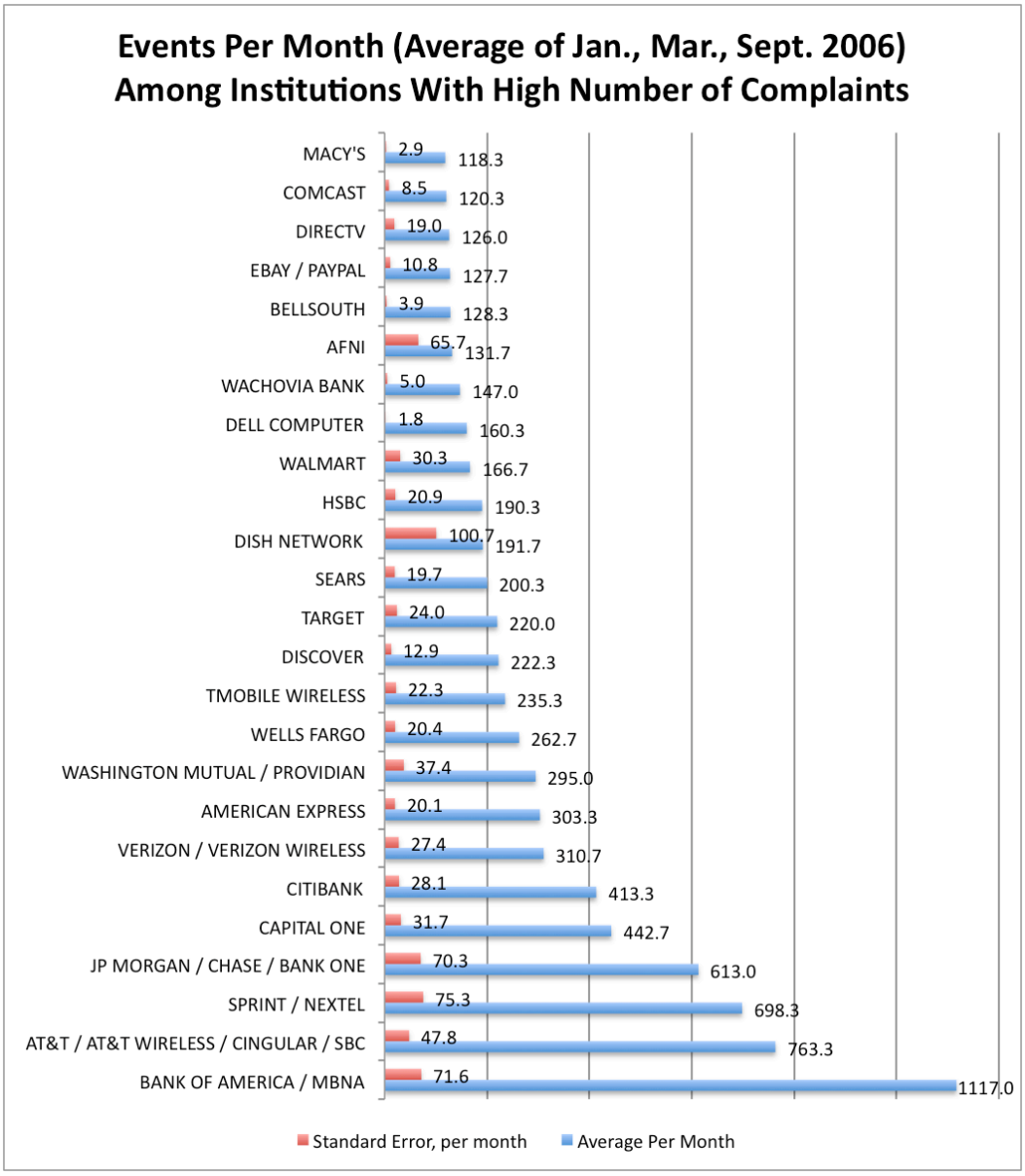
[48] See e.g., WELLS FARGO BANK, GLBA INFORMATION SHARING STUDY COMMENT, Apr. 23, 2002, available at www.ots.treas.gov/docs/r.cfm?95404.pdf.

[49] 21 Harv. J. L. Tech. 97 (2007), *available at* http://jolt.law.harvard.edu/articles/pdf/v21/HOOFNAGLE_Identity_Theft.pdf.

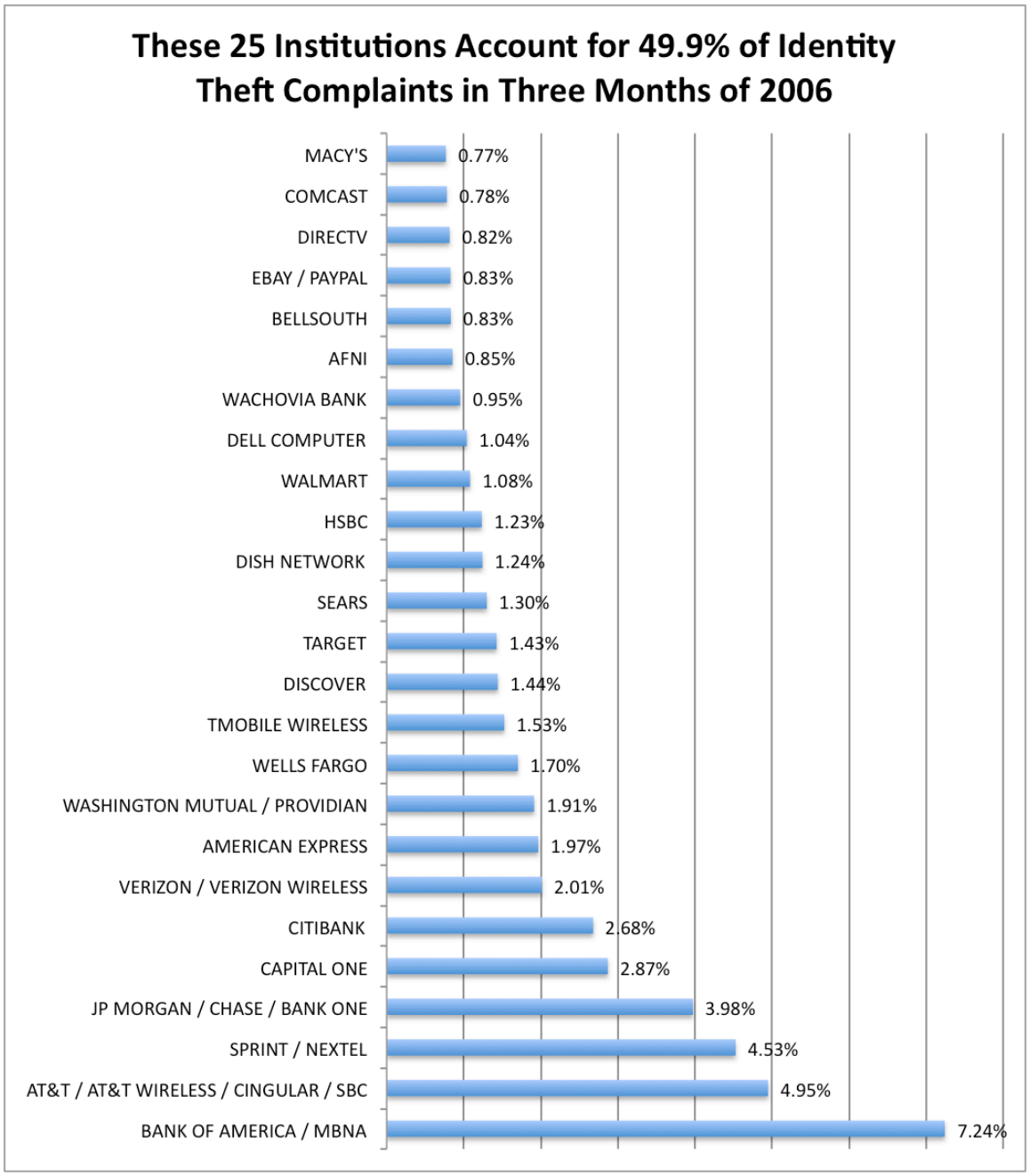
Results and Discussion

Top 25 Institutions by Number of Fraud Events

Bank of America ranks highest in total number of events. Given that this institution is the largest among US banks for deposits, and the resulting concentration of attacks against it by impostors, it is not surprising that it ranks so highly in overall events. Bank of America was followed by two telecommunications carriers, AT&T and Sprint/Nextel. Other major telecommunications carriers were present in the top fifteen when ranked by total number of events.

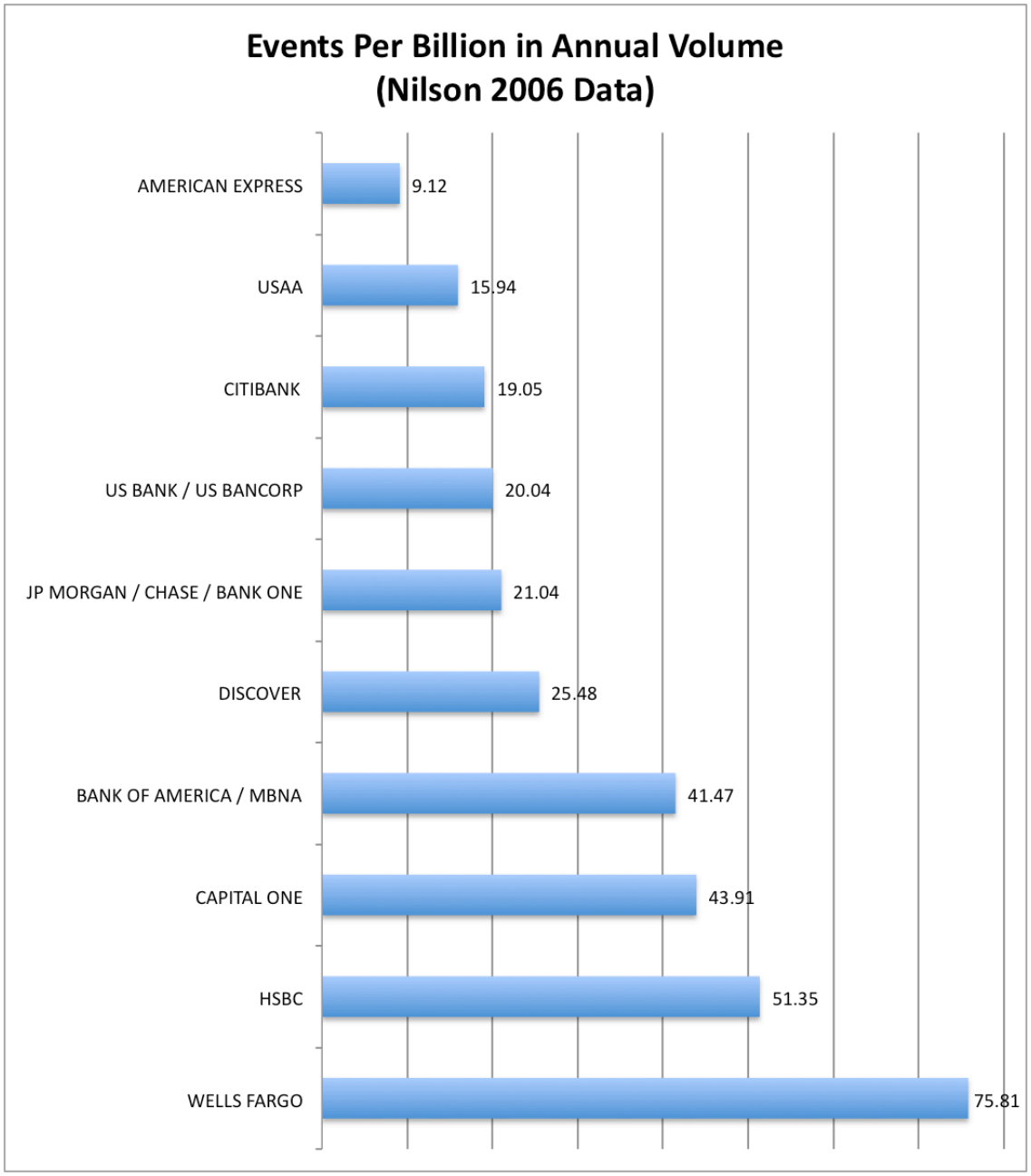


These 25 institutions, taken together, accounted for almost 50% of all identity theft events over three months of FTC data in 2006. With these statistics, FTC and law enforcement can focus their efforts on the biggest targets of impostors.



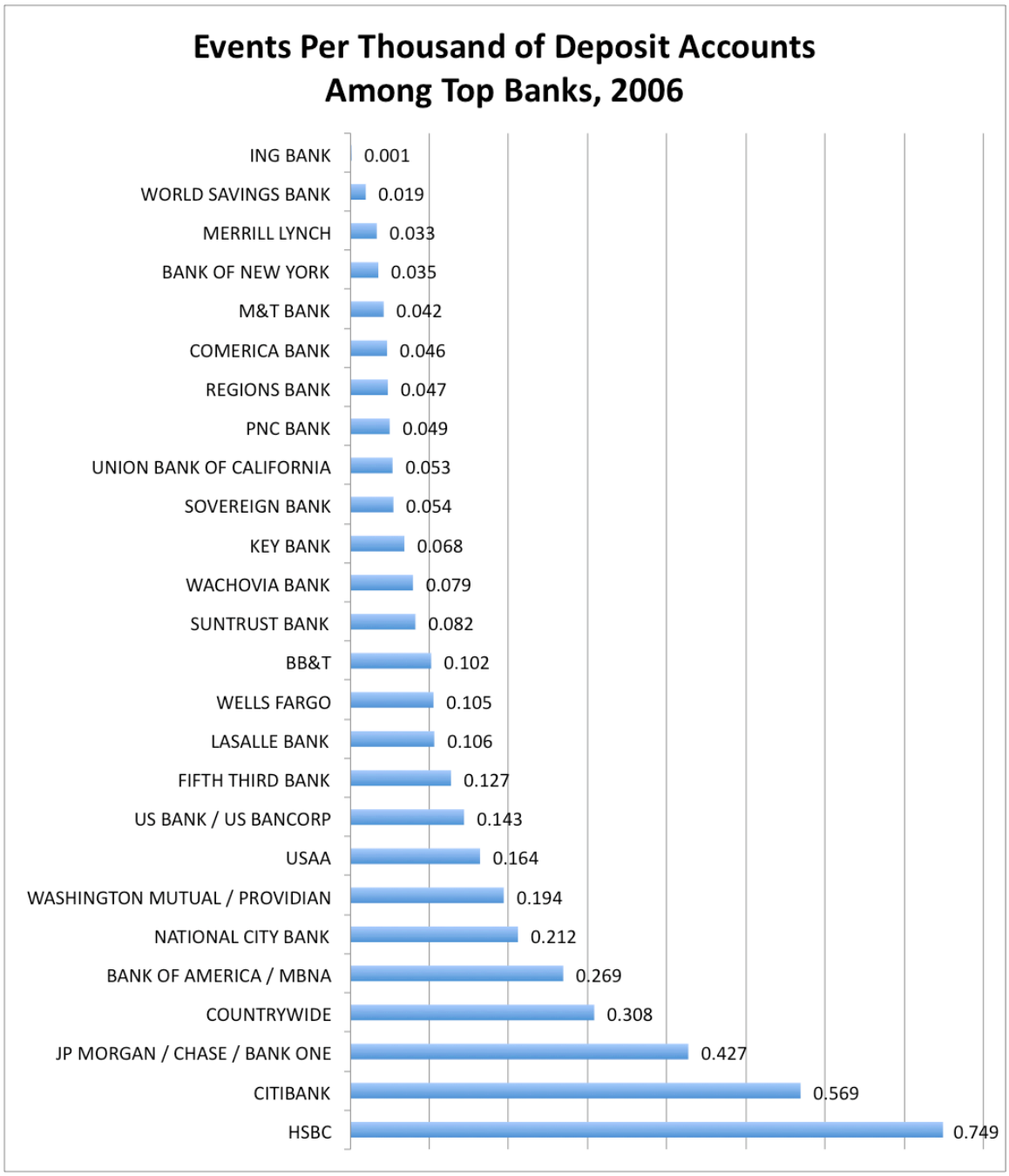
Top Credit Card Issuers By Volume, 2006

When the estimated annual events are applied to the top ten credit card issuers according to the Nilson Report, by volume of cash advances and purchases made in 2006, American Express emerges as the least likely to suffer an identity theft event, followed by USAA. While Bank of America ranked highly in overall events, adjusting for credit card volume, Wells Fargo, HSBC, and Capital One emerge at the top.



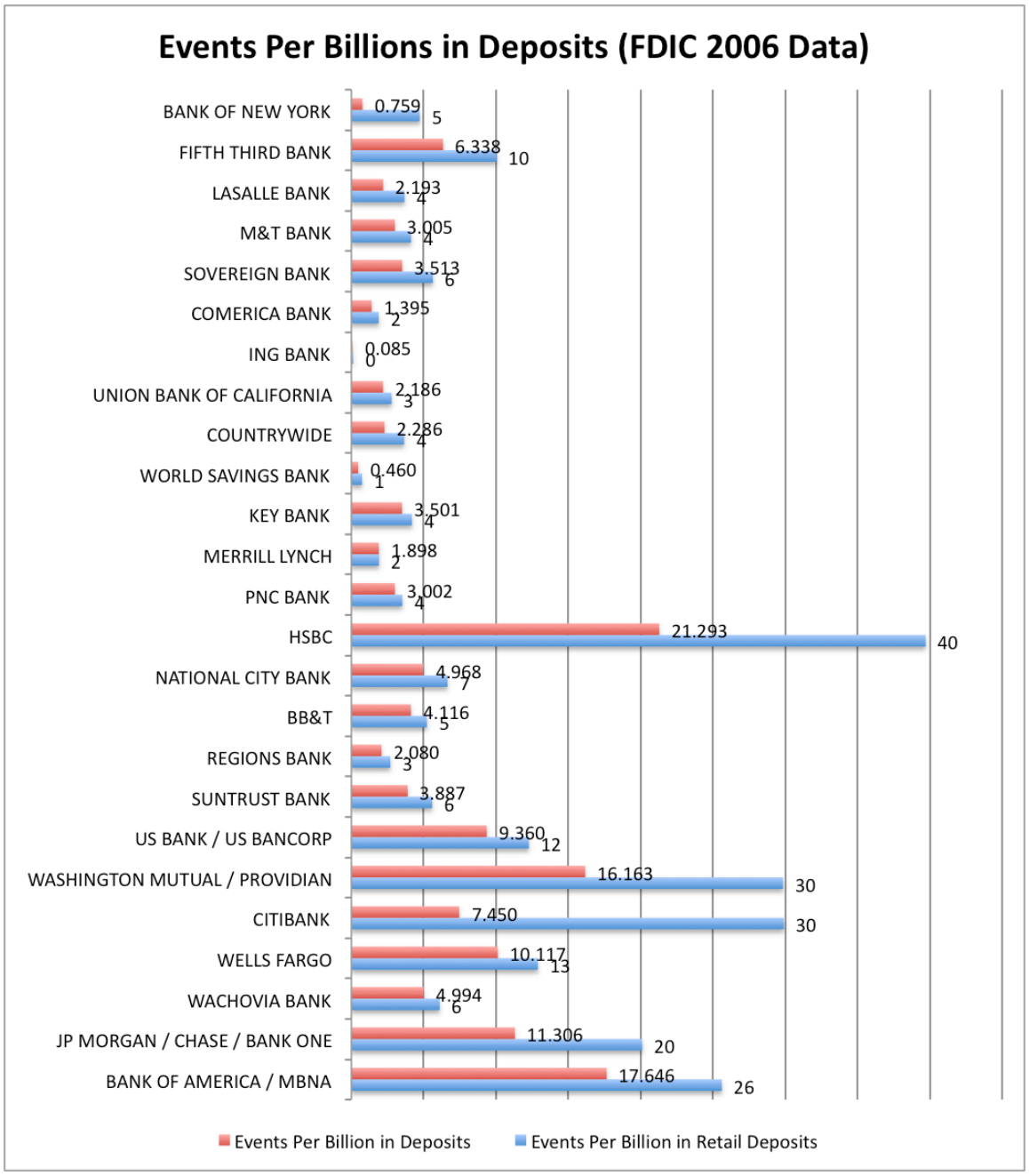
Top Banks Ranked By Number of Deposit Accounts in 2006

Each year, financial institutions report the number of depository accounts they maintain in a June "Call" report. This chart presents the estimated annual events per thousand depository accounts. ING Bank has the lowest rate of fraud under this measure, while institutions with large credit card portfolios rank highly.



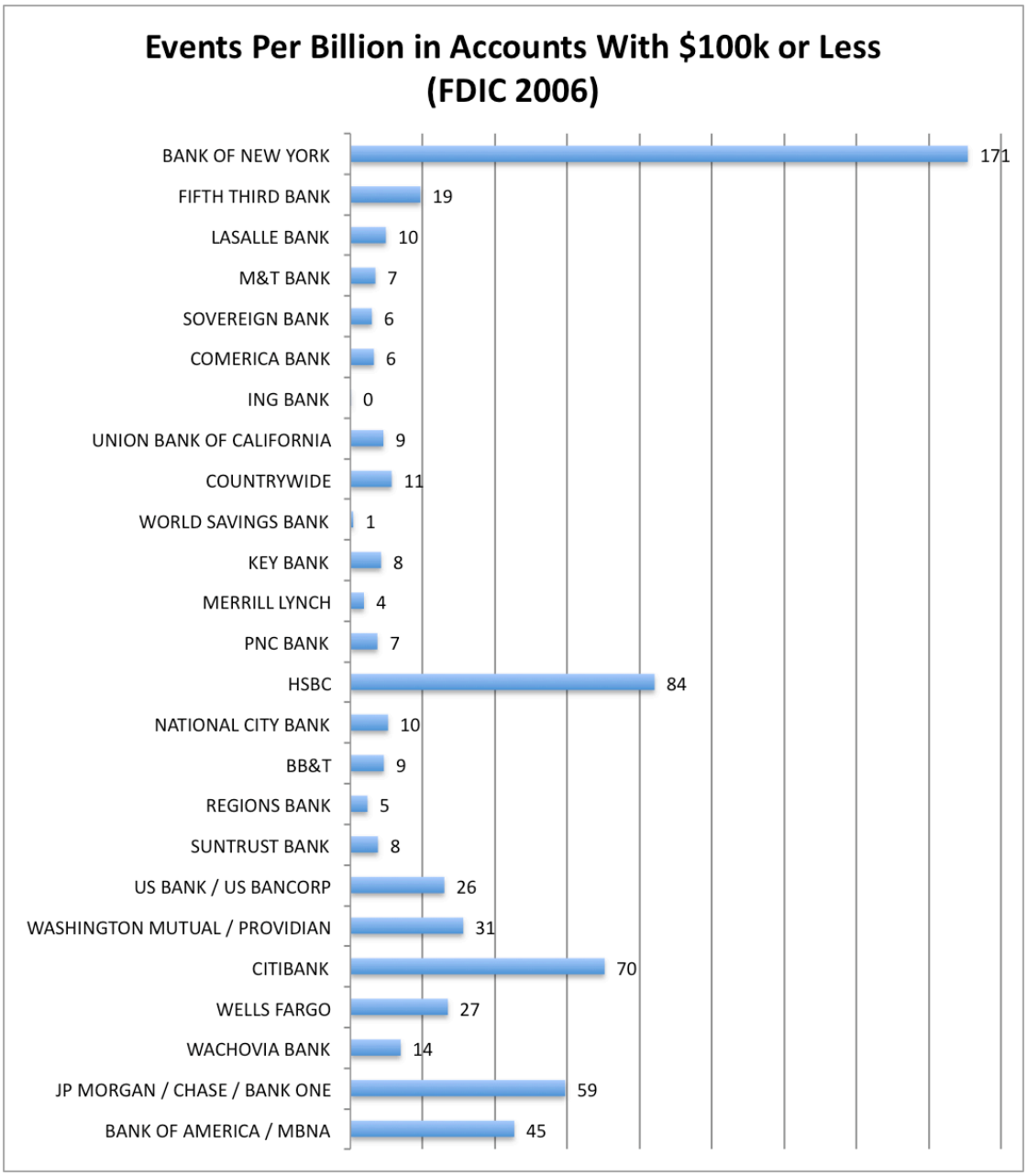
Top Financial Institutions by Deposits

Version 1.0 compared banks by total deposits. This version adds a new comparison tool—"retail deposits," a measure that should eliminate some large corporate accounts. ING Bank, with only a single event, had the lowest incidence of identity theft under both measures. HSBC, Washington Mutual, and Bank of America perform poorly on both measures. This chart orders the top 25 banks from smallest to largest, based on total deposits.



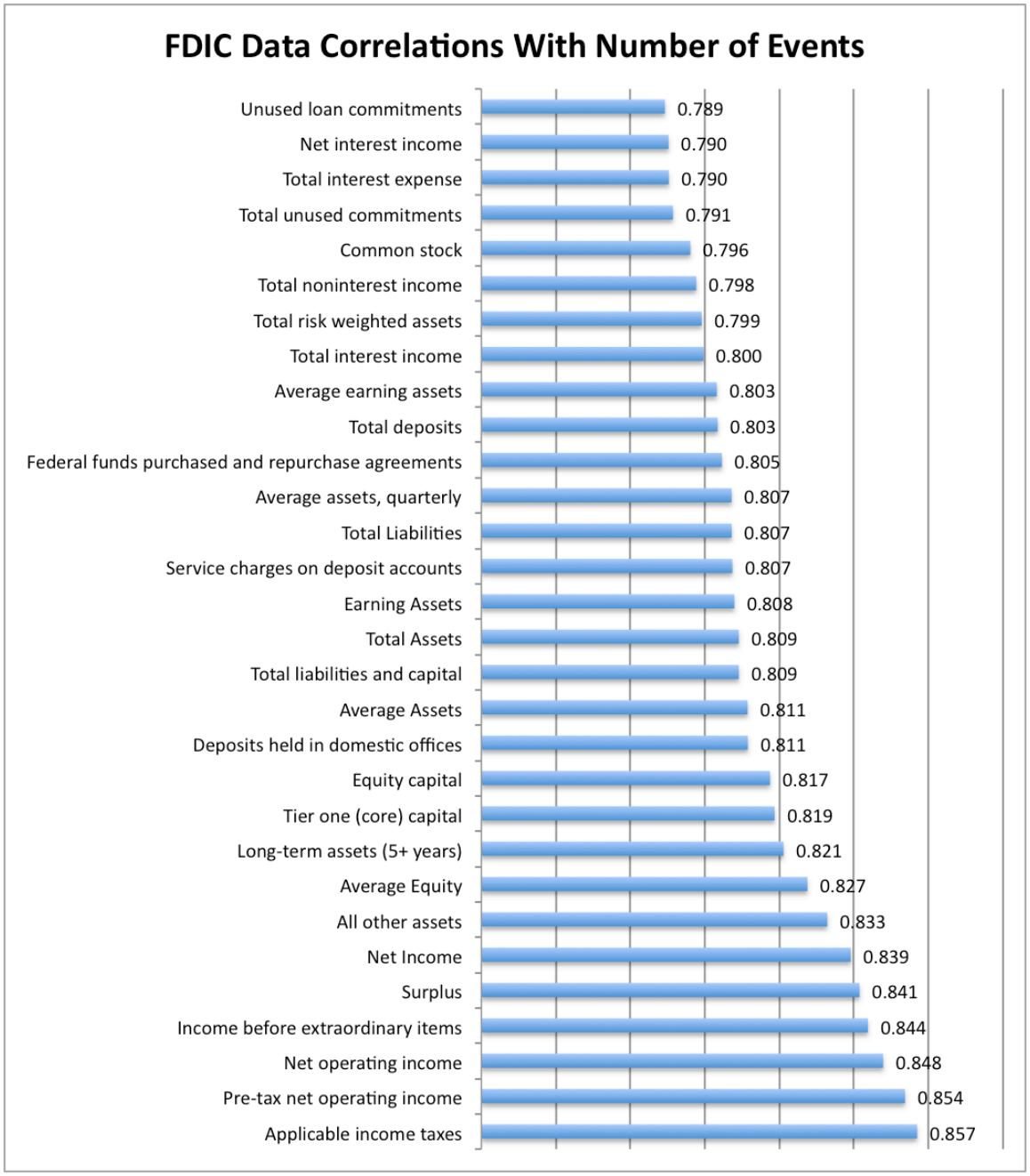
Top Financial Institutions By Accounts Under $100,000

When compared on deposits in accounts with $100,000 or less, Bank of New York emerges as a strong outlier here. This finding should be discounted because this bank only had eight reported events in the three months sampled, its depository footprint under this measure is extremely small, and because this same bank performed very well under other metrics. That institution is followed by HSBC, Citibank, JP Morgan Chase, and Bank of America.



Correlation Analysis

A correlation analysis shows a strong link between measures of institution size and number of events. This could mean that larger institutions are targeted successfully more frequently, or that larger institutions are less effective in preventing identity theft events. The top correlating statistics of the largest banks from the FDIC SDI database are presented below.



Other Observations

Several commenters referred to Bank of America's pilot program to provide credit cards to undocumented individuals as a risky endeavor. The Wall Street Journal reported on this program in February 2007:

> *The new Bank of America program is open to people who lack both a Social Security number and a credit history, as long as they have held a checking account with the bank for three months without an overdraft. Most adults in the U.S. who don't have a Social Security number are undocumented immigrants.*[50]

Contrary to the commenters objections, the Bank of America pilot appears to be one that be useful in finding approaches to reduce fraud, especially check kiting, synthetic identity theft, and new account frauds that rely upon instant credit. Requiring a three-month waiting period before entertaining an application for a card eliminates the fast reward provided to impostors exploiting credit offers. If statistics were reported on Bank of America's program, regulators and the public could focus on the efficacy in waiting periods in preventing identity theft.

While this analysis focused on financial institutions, in processing the data, it is clear that a similar analysis should be performed on utility companies. Thousands of victims identified various utilities companies as the institution involved in the fraud. Generally speaking, there is a lower level of customer authentication in the establishment of utilities service, and impostors may bootstrap these accounts in order to obtain accounts at other organizations.[51]

Telecommunications companies figured prominently in the overall event count. Lacking a meaningful metric to assess the size of these institutions, it is impossible to compare telecommunications companies to each other or to financial institutions. It is clear, however, that consumers would benefit from heightened attention being focused

---

[50] Miriam Jordan & Valerie Bauerlein, *Bank of America Casts Wider Net For Hispanics; Lender Risks Controversy Aiming New Credit Card At Illegal Immigrants*, Wall Street Journal, Feb. 13, 2007, *available at* http://online.wsj.com/article_print/SB117133501870406767.html

[51] Jennifer Barrett, Chief Privacy Officer, Acxiom, Remarks at Security in Numbers, SSNs and ID Theft, Federal Trade Commission Workshop (Dec. 10, 2007), *available at* http://www.ftc.gov/bcp/workshops/ssn/index.shtml.

upon identity theft events at carriers. The next version of this report will explore various metrics to compare telecommunications carriers.

Conclusion

This paper began with a metaphor concerning the revolution in automobile safety experienced over the last 50 years. At the beginning of the 1960s automobile safety debate, a blame the driver mentality stood in the way of a nuanced understanding of the problem, and consumers lacked reliable measures for comparing cars on safety. We are in similar posture today with respect to identity theft. Identity theft is a problem, like automobile accidents, that will never be completely solved. Individuals, inexperienced as they are with technology and new methods of payment, will undoubtedly continue to contribute to the problem. If we are to develop a consumer market for bank safety comparable to automobile safety, we need to acknowledge these problems and find ways to foster vigorous competition among institutions for prevention of identity theft. This effort seeks to enhance competition through providing consumers with reliable metrics to compare incidence of identity theft among institutions. If data were available on this crime, consumers could choose safer institutions, regulators could focus attention on problem actors, and businesses themselves could compete to protect consumers from this crime.

According to the measures employed in this analysis, American Express, USAA, and Citibank have the lowest rate of identity theft events in 2006 among top credit card issuers. Among consumer banks, ING Bank and World Savings Bank performed well in 2006 under every measure. Correlations were calculated for all the statistics the Federal Deposit Insurance Corporation maintains on top banks; generally the number of identity theft events correlates strongly with measures of institutions size.

This is an ongoing, imperfect attempt to quantify risk of identity theft among institutions. Several methodological challenges are explained in the methods section, but the most obvious improvement upon this effort would be institution of voluntary, public reporting by institutions themselves on identity theft. The author welcomes constructive criticism, suggestions, and comments in an effort to create a more perfect picture of identity theft.

Appendix A: Top 50 Institutions by Total Events (Jan., Mar., Sept. 2006)

Institution Name	Incidents Per Billion in Deposits	Extrapolated to 12 Months	Total Events, 3 Months	% of 3 Months (46262 events)	Total Deposits +$000 (12/31/06)
BANK OF AMERICA / MBNA	17.646	13404	3351	7.24%	759,600,625
AT&T / AT&T WIRELESS / CINGULAR / SBC		9160	2290	4.95%	
SPRINT / NEXTEL		8380	2095	4.53%	
JP MORGAN / CHASE / BANK ONE	11.306	7356	1839	3.98%	650,614,000
CAPITAL ONE	242.126	5312	1328	2.87%	21,939,005
CITIBANK	7.450	4960	1240	2.68%	665,743,000
VERIZON / VERIZON WIRELESS		3728	932	2.01%	
AMERICAN EXPRESS	485.769	3640	910	1.97%	7,493,273
WASHINGTON MUTUAL / PROVIDIAN	16.163	3540	885	1.91%	219,019,003
WELLS FARGO	10.117	3152	788	1.70%	311,546,000
TMOBILE WIRELESS		2824	706	1.53%	
DISCOVER	106.021	2668	667	1.44%	25,164,842
TARGET		2640	660	1.43%	
SEARS		2404	601	1.30%	
DISH NETWORK		2300	575	1.24%	
HSBC	21.293	2284	571	1.23%	107,265,046
WALMART		2000	500	1.08%	
DELL COMPUTER		1924	481	1.04%	
WACHOVIA BANK	4.994	1764	441	0.95%	353,234,000
AFNI		1580	395	0.85%	
BELLSOUTH		1540	385	0.83%	
EBAY / PAYPAL		1532	383	0.83%	
DIRECTV		1512	378	0.82%	
COMCAST		1444	361	0.78%	
MACY'S		1420	355	0.77%	
ASSET ACCEPTANCE		1348	337	0.73%	
JC PENNEY		1348	337	0.73%	
US BANK / US BANCORP	9.360	1272	318	0.69%	135,903,121
NCO		1052	263	0.57%	
EQUIFAX		1008	252	0.54%	
YAHOO		940	235	0.51%	
HOME DEPOT		908	227	0.49%	
TRANSUNION		816	204	0.44%	

LOWE'S		788	197	0.43%	
EXPERIAN		780	195	0.42%	
BEST BUY		740	185	0.40%	
PACIFIC BELL		716	179	0.39%	
TRS RECOVERY		716	179	0.39%	
QWEST		700	175	0.38%	
MCI		656	164	0.35%	
ALLIED INTERSTATE COLLECTIONS		620	155	0.34%	
GE		588	147	0.32%	
SOUTHWESTERN BELL		552	138	0.30%	
FINGERHUT		536	134	0.29%	
MIDLAN CREDIT		508	127	0.27%	
COX CABLE		504	126	0.27%	
SUNTRUST BANK	3.887	492	123	0.27%	126,571,181
NATIONAL CITY BANK	4.968	432	108	0.23%	86,954,966
BB&T	4.116	344	86	0.19%	83,585,119
FIFTH THIRD BANK	6.338	248	62	0.13%	39,126,022

Appendix B: Top Banks and Credit Card Issuers Under New Measures

Institution Name	Total Events, 3 Months	% of 3 Months (46262 events)	Extrapolated to 12 Months	Incidents Per Billion in Deposits	Total Deposits +$000 (12/31/06)	Incidents Per Billion in Retail Deposits	Retail deposits +000	Incidents Per Billion in Accounts w/ 100k or less	Deposit accounts of $100,000 or less +$000	Incidents Per Billion in Volume, 2006	Nilson, Highest Volume 2006 Cash & Purchases +000	Incidents Per Billion in Outstandings ,2006	Nilson, Top Issuers of General Cards, 2006 Outstandings +000
WELLS FARGO	788	1.70%	3152	10.117	311,546,000	13	244,503,000	27	116,905,000	75.806	41,580,000	151.030187	20,870,000
HSBC	571	1.23%	2284	21.293	107,265,046	40	57,517,560	84	27,141,097	51.349	44,480,000	81.2522234	28,110,000
CAPITAL ONE	1328	2.87%	5312	242.126	21,939,005	810	6,557,420	712	7,461,403	43.912	120,970,000	88.9037657	59,750,000
BANK OF AMERICA / MBNA	3351	7.24%	13404	17.646	759,600,625	26	523,303,268	45	295,673,999	41.469	323,230,000	88.4460574	151,550,000
DISCOVER	667	1.44%	2668	106.021	25,164,842	618	4,318,552	1,582	1,686,533	25.482	104,700,000	58.4446878	45,650,000
JP MORGAN / CHASE / BANK ONE	1839	3.98%	7356	11.306	650,614,000	20	365,834,000	59	123,792,000	21.042	349,590,000	49.7531282	147,850,000
US BANK / US BANCORP	318	0.69%	1272	9.360	135,903,121	12	103,673,650	26	48,971,299	20.041	63,470,000	99.7647059	12,750,000
CITIBANK	1240	2.68%	4960	7.450	665,743,000	30	165,840,000	70	70,519,000	19.048	260,390,000	45.2968037	109,500,000
USAA	98	0.21%	392	1247.426	314247	9,190	42,655	9,376	41,810	15.941	24,590,000		
AMERICAN EXPRESS	910	1.97%	3640	485.769	7,493,273	1,152	3,160,368	1,152	3,160,366	9.123	398,990,000	43.8554217	83,000,000
WACHOVIA BANK	441	0.95%	1764	4.994	353,234,000	6	288,971,000	14	126,902,000				
WASHINGTON MUTUAL / PROVIDIAN	885	1.91%	3540	16.163	219,019,003	30	118,594,990	31	113,409,271			150.638298	23,500,000
SUNTRUST BANK	123	0.27%	492	3.887	126,571,181	6	88,141,703	8	64,716,199				
REGIONS BAN	53	0.11%	212	2.080	101,916,668	3	78,741,751	5	45,078,620				
BB&T	86	0.19%	344	4.116	83,585,119	5	65,897,515	9	37,211,691				
NATIONAL CIT	108	0.23%	432	4.968	86,954,966	7	65,014,506	10	41,540,729				
PNC BANK	49	0.11%	196	3.002	65,279,906	4	55,687,897	7	26,297,199				
MERRILL LYNC	26	0.06%	104	1.898	54,805,257	2	54,568,050	4	27,763,746				
KEY BANK	54	0.12%	216	3.501	61,704,552	4	51,582,966	8	25,480,749				
WORLD SAVIN	8	0.02%	32	0.460	69,603,422	1	43,674,196	1	41,061,441				
COUNTRYWID	32	0.07%	128	2.286	55,987,217	4	35,107,904	11	11,225,898				
UNION BANK (	24	0.05%	96	2.186	43,916,662	3	34,518,785	9	10,529,238				
ING BANK	1	0.00%	4	0.085	47,219,297	0	34,237,100	0	34,237,100				
COMERICA BA	16	0.03%	64	1.395	45,884,035	2	33,911,938	6	9,856,871				
SOVEREIGN B	45	0.10%	180	3.513	51,244,655	6	31,951,654	6	30,347,316				
M&T BANK	30	0.06%	120	3.005	39,939,021	4	29,100,798	7	17,417,863				
LASALLE BANK	24	0.05%	96	2.193	43,783,215	4	26,150,735	10	9,798,752				
FIFTH THIRD BANK	62	0.13%	248	6.338	39,126,022	10	24,711,831	19	12,793,226				
BANK OF NEW	12	0.03%	48	0.759	63,258,000	5	10,160,000	171	281,000				
STATE STREET	2	0.00%	8	0.120	66,560,064	6	1,248,701	78	102,230				