Measuring Identity Theft at Top Banks (Version 1.0)

Victim Data Shows High Relative Incidence of Fraud Among Top Financial Institutions, Many Events At Telecom Carriers in 2006

February 26, 2008

By Chris Jay Hoofnagle[1]

Abstract

There is no reliable way for consumers, regulators, and businesses to assess the relative incidence of identity fraud at major financial institutions. This lack of information prevents more vigorous competition among institutions to protect accountholders from identity theft. As part of a multiple strategy approach to obtaining more actionable data on identity theft, the Freedom of Information Act was used to obtain complaint data submitted by victims in 2006 to the Federal Trade Commission. This complaint data identifies the institution where impostors established fraudulent accounts or affected existing accounts in the name of the victim. The data show that some institutions have a far greater incidence of identity theft than others. The data further show that the major telecommunications companies had numerous identity theft events, but a metric is lacking to compare this industry with the financial institutions.

This is a first attempt to meaningfully compare institutions on their performance in avoiding identity theft. This analysis faces several challenges that are described in the methods section. The author welcomes constructive criticism, suggestions, and comments in an effort to shine light on the identity theft problem (choofnagle@law.berkeley.edu).

---

[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

Consumers, regulators, and businesses lack objective tools to compare incidence of identity theft[2] across financial and other institutions targeted by fraudsters. Without such tools, consumers cannot "vote with their feet" and choose safer institutions, regulators cannot allocate oversight and enforcement resources to high-risk institutions and practices, and businesses themselves cannot assess how well they perform relative to competitors in fighting this crime. While competition is a powerful force for consumer protection, the lack of information about identity theft makes the market less effective in creating a race to the top among institutions to shield consumers from fraud.

To address these problems, lending institutions should publicly report basic statistical information about identity theft events.[3] Specifically, they should report 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.

In absence of such reporting, actors in the market must rely upon other, more imperfect sources of information to assess the risk of identity theft. None of these existing sources provides any information on the relative incidence of fraud among institutions. Some sources of information may be misleading. For instance, one institution that has broadcast humorous commercials about its efforts to prevent identity

---

[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] *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.

theft ranks highly in this analysis for both overall number of events and relative incidence of the crime.[4]

As part of a multiple strategy approach to obtaining more actionable data on identity theft, 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. After aggregating and manipulating the complaint data according to the relative sizes of the institutions, the data show that some institutions have a far greater incidence of identity theft than others. The data further show that the major telecommunications companies had numerous identity theft events, but a metric is lacking to compare this industry with the financial institutions.

This analysis faces several challenges that are described in the methods section below. This is a first attempt—a work in process—to meaningfully compare institutions on their performance in avoiding identity theft. The author welcomes 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

The FTC collects information from identity theft victims by phone and through an online form.[5] 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

---

[4] See e.g, Citibank Identity Theft Commercial, available at http://www.youtube.com/watch?v=KERwnA8VfFM.

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

institutions identified by victims.[6] 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 thousands of complaints (the FTC received 674,354 complaints in 2006; 246,035 were identity theft related[7]), 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.

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 (i.e., Wallmart, Citybank, Bank of American), combined where companies that, as of 2006, were merged but nevertheless were identified as separate companies by consumers (i.e., AT&T Wireless and Cingular, JP Morgan and Chase), and consolidated when corporate names were merged with a specific product (i.e., "Citibank Visa" became "Citibank").

---

[6] *See* FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2007 (Feb. 2008).

[7] FEDERAL TRADE COMMISSION, CONSUMER FRAUD AND IDENTITY THEFT COMPLAINT DATA, JANUARY – DECEMBER 2006 (Feb. 2007).

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

Valid entries were ranked by number of events and relative incidence of fraud by institution. Institutions were ranked by size according to their total deposits in December 2006, according to the FDIC's SDI Database.[8] Incidence 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. This means that the number of fraud events are 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 incidence of identity theft.

Challenges in Measuring Frequency and Rates of Fraud

Several methodological challenges must be understood in order appreciate what this analysis shows and how it could be improved.

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

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."[9] This may especially be the case with account takeovers, because many victims resolve the issue with a call to the institution without further inconvenience.[10] "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,"[11] may not be reflected by consumer complaints. As a result, this analysis undercounts the total number of identity theft events in the months analyzed.

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.[12] 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.[13] Accordingly, information distinguishing between account takeovers and new

---

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

[10] 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).

[11] FEDERAL TRADE COMMISSION – IDENTITY THEFT SURVEY REPORT (Nov. 2007).

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

[13] 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.

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.

For purposes of determining relative incidence of fraud, the size of institutions was assessed by total deposits, according to the FDIC SDI database. Total deposits includes: "The sum of all deposits including demand deposits, money market deposits, other savings deposits, time deposits and deposits in foreign offices." Larger institutions with significant corporate and business accounts may appear to have a lower incidence than smaller banks that are primarily consumer-focused under this measure. A better measure would be number of customers, or number of accounts, however, that information is not publicly available.

At present, we lack a reliable method to assess the size of the telecommunications carriers, and this is problematic because these institutions ranked so highly in overall number of complaints. As a result, no analysis of relative incidence is performed between carriers and banks, or among carriers themselves.

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." If all of Citibank's fraud events are allocated under the first, the institution's fraud rate is 7.45 per billion in deposits; if under the latter, it is 181.23 per billion in deposits.

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

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.

Finally, this report relies upon 2006 data, the most recent available, because of the delay associated with requesting information under the Freedom of Information Act. 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.

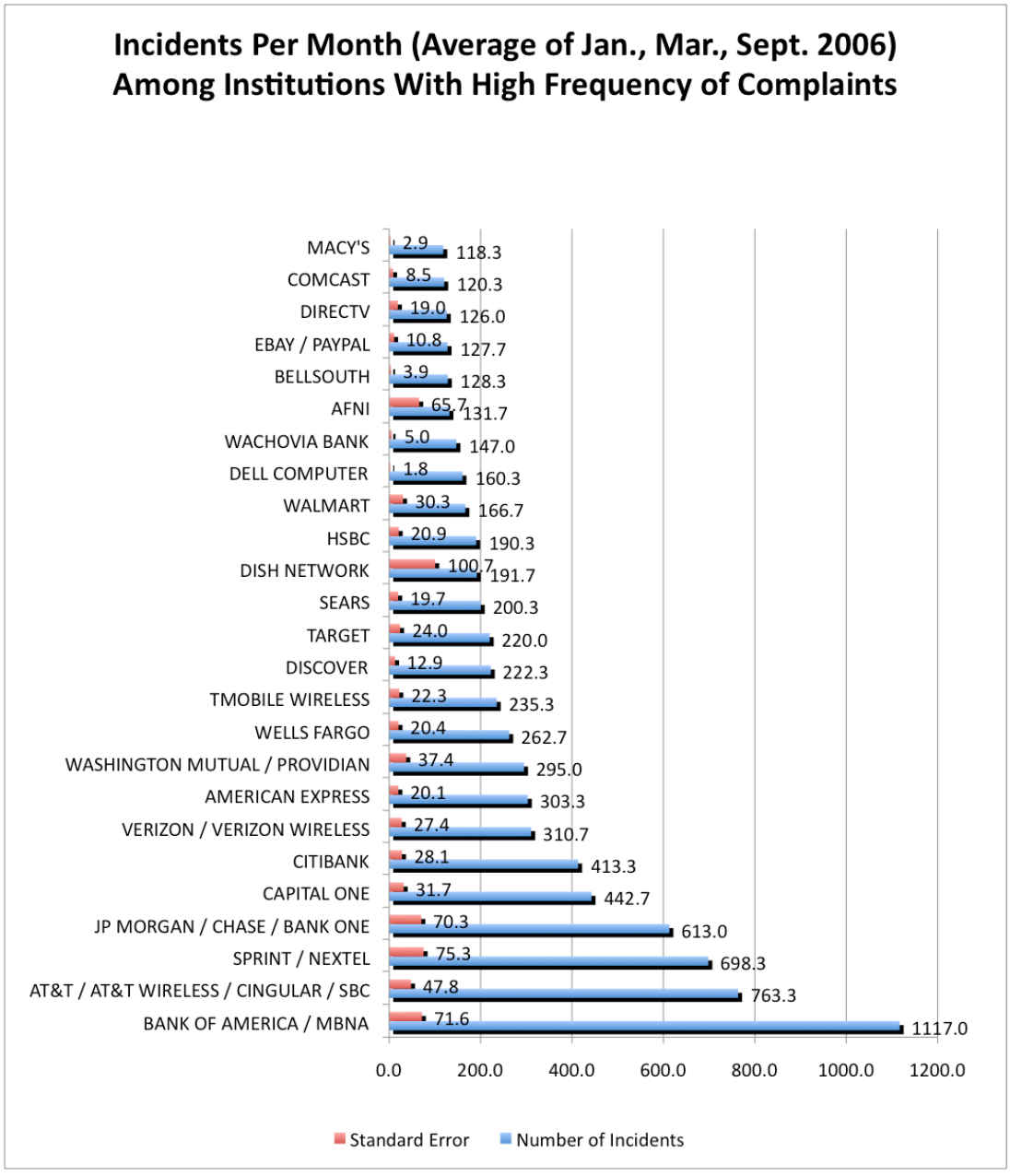
Taken together, these limits point to the need for identity theft reporting by institutions themselves, as outlined in *Identity Theft: Making the Unknown Knowns Known.*[14] A more complete picture of identity theft will not emerge until institutions provide more transparency on the problem.

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

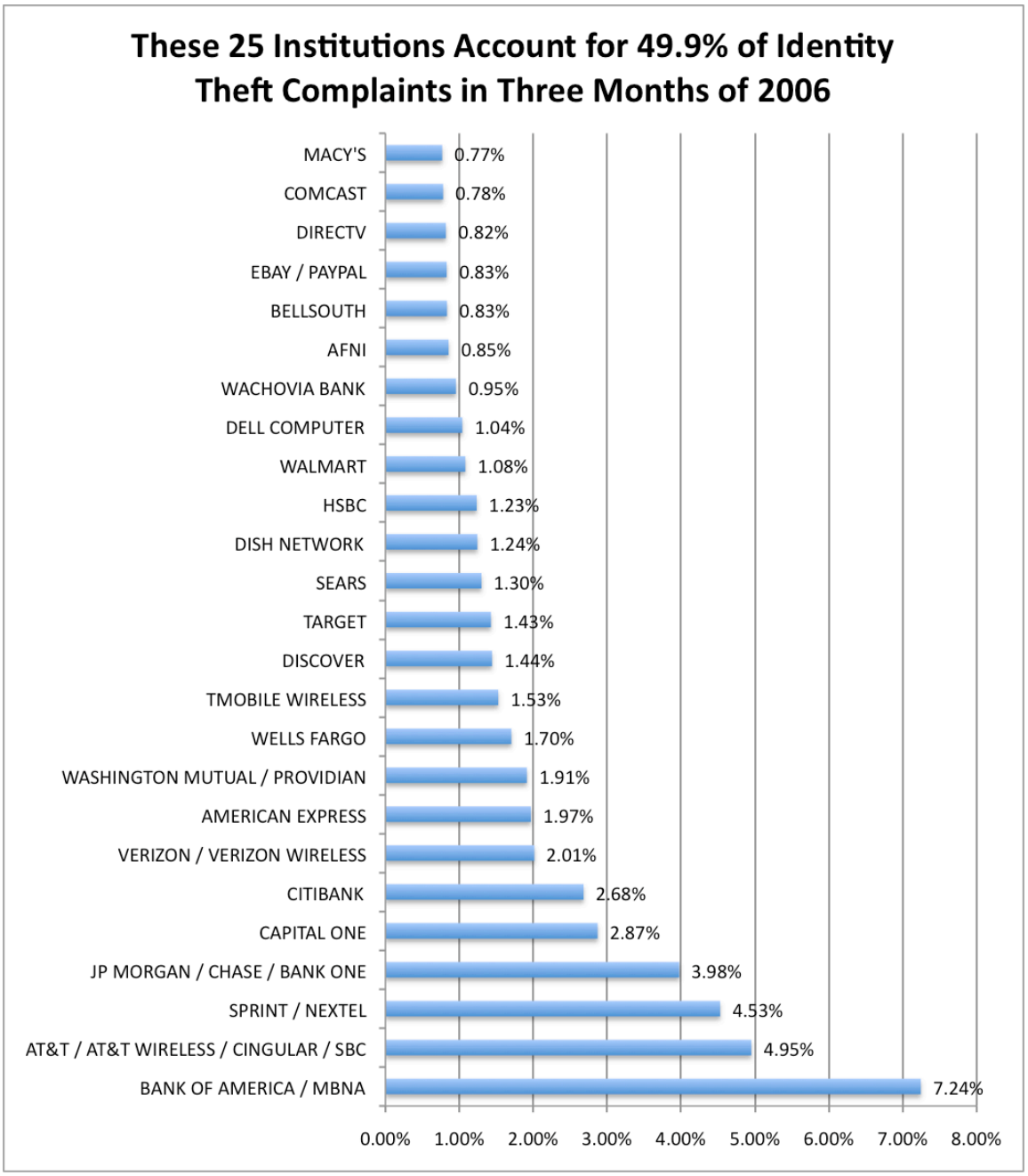
Results and Discussion

Top 25 Institutions by Frequency of Complaints

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.

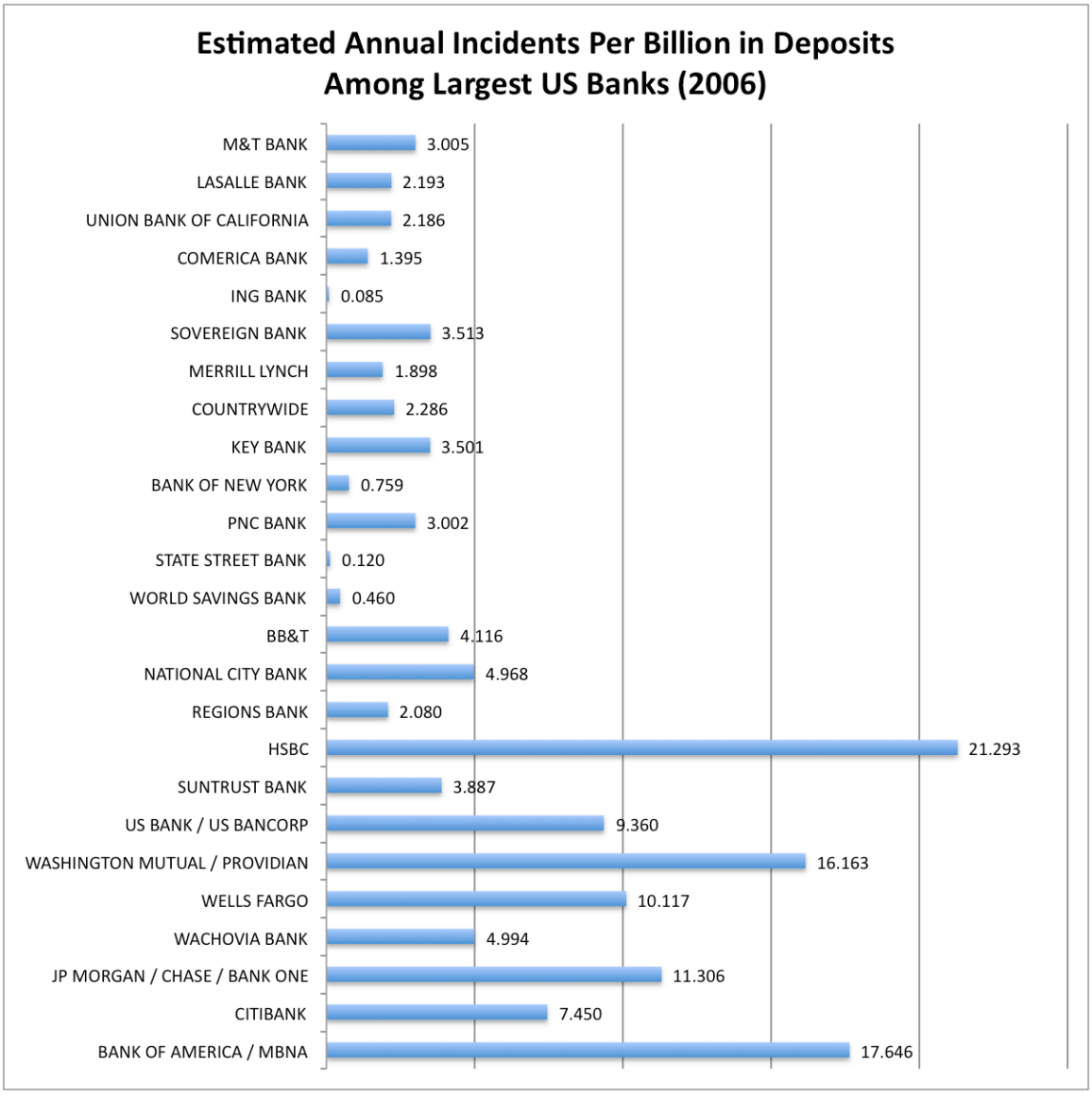


These 25 institutions, taken together, accounted for almost 50% of all identity theft events over three months of FTC data in 2006. With these statistics, FTC and law enforcement can focus their efforts on the biggest targets of impostors.



Top Financial Institutions by Size

Among the largest financial institutions, when the estimated events are divided by total deposits, the data show that HSBC has a higher incidence of fraud than Bank of America. ING Bank, with only a single event, had the lowest incidence of identity theft. This chart orders the top 25 banks from smallest to largest, based on deposits.



Other Observations

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 upon identity theft events at carriers.

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.

Conclusion

In order for the market to effectively address the ongoing identity theft epidemic, consumers need reliable information about incidence of the crime 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.

This analysis shows that some institutions have a far greater incidence of identity theft than others. The data further show that the major telecommunications companies had numerous identity theft events, but a metric is lacking to compare this industry with the financial institutions.

This is a first, imperfect attempt in quantifying 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