International Review of Business Research Papers
Vol.6, No.1 February 2010, Pp.135-144

Identity Theft Issues for Financial Services Firms

John W. Moore*

Financial services firms are the targets of 30% of phishing email attacks intended to steal customers' identities and the assets in their accounts. Last year, 285 million records were compromised in data breaches in the US; many of these were linked to organized crime. On the Internet, websites operated expressly for criminals buying and selling stolen credit cards details, bank account credentials, and stolen identities are operated by organized crime. Consequences of this identity theft phenomenon can be severe for both financial institutions and their customers – monetary losses in lawsuits, card reissue costs, and making debit/credit cardholders whole, as well as customers' out-of-pocket costs, the hours spent resolving it, and the customer churn and brand devaluation that usually follow. This paper discusses the threats posed to the payment system, the Internet mechanism used to sell stolen digital assets, and new work that identifies the top banks' incidents of identity theft as reported to the Federal Trade Commission. It includes explanation of how such events are carried out, and provides suggestions to help reduce the risks to financial firms.

Field of Research: Contemporary Issues in Banking

1.0 Introduction

Many people do not know how their online identities were stolen, but others do – breaches of company computer security to steal the account information within are reported on a depressingly frequent basis. Hackers tricking customers of legitimate businesses into revealing their personally identifiable information likewise are frequent revelations in the news. Identity theft used to be carried out on a small scale by hackers

* Prof. John W. Moore, School of Business and Technology, University of Maryland Eastern Shore email: jwmoore1@umes.edu

looking for bragging rights, but no more. Identity theft is organized, large-scale, and performed by some very skilled criminals who are members of organized crime rings.

2.0 Literature Review

Identity theft poses a major threat to commerce because it threatens the integrity and efficiency of the payment system. Schreft (2007) identified market failures to price in the cost of the risk of expected misuse of personally identifiable information (PII) as a major issue. There is little incentive for organizations to provide more than a minimum level of security for protection of PII. Sellers providing strong security bear the full cost but because of price competition from sellers with weak security (and low security investment) are unable to recover the costs. Another issue revolves around external partners in transaction processing; as demonstrated by the Heartland Payment Processors debacle in February, the network that processes consumer transactions is only as strong as its weakest link. Finally, due to the public's response to security issues, trust in the payment system is threatened. Because consumers fear becoming victims of identity theft, more rigorous authentication is required, impairing efficiency in completing transactions. Some consumers react to the lack of integrity in the payment system by not adopting or discontinuing use of some forms of payment, so efficiency declines.

If the efficiency of the payment system is any doubt, similar worries do not appear to impede the worldwide market for stolen identities. Peretti (2009) described the evolution of the carding websites used to facilitate the buying and selling of stolen financial and personal information. Carding refers to "…an assortment of activities surrounding the theft and fraudulent use of credit and debit card account numbers including computer hacking, phishing, cashing-out stolen account numbers, reshipping schemes, and Internet auction fraud." (p. 380) A number of websites devoted to these activities are discussed(example: www.theftservices.com). Among the features of these sites are tutorials, message boards for posting wanted or for sale blocks of account numbers, tools for constructing false web pages of commercial firms, and lists of members caught stealing from each other. Peretti notes that some of these sites have had membership in the thousands.

Symantec's Global Internet Security Threat Report (2009a) provides support for Peretti's paper on carding forums. In its examination of the underground economy, Symantec discovered the number one item (by volume) being sold was credit card information, accounting for 32% of the traffic. Price ranges for credit cards ranged between $0.06 and $30 each. The second most popular item were bank account credentials, with 19% of the traffic. Depending on the value of the accounts, prices ranged from $10 to $1,000. Complete identities, at 4% of the traffic, were priced from $0.70 to $60.

Despite the public awareness of identity theft, and its use in stealing financial assets, consumers of banking and financial products have not been able to identify which institutions were best able to defeat identity theft. Hoofnagle (2008) published the first study of identity theft at large US banks. Using the Federal Trade Commission's 2006 victim complaint data with an FOI request, he found that there was a wide disparity between the banks' numbers of identity theft complaints. For three randomly selected months in 2006, he identified 25 business organizations (13 bank/financial services, five retailers, and eight telecom/internet providers) that represented 49.9% of the FTC's identity theft complaints for the period. In terms of the absolute number of complaints, three firms represented almost 17% of all complaints (Bank of America, 7.24%; AT&T, 4.95%; and Sprint (4.53%). For banks, when size was considered (estimated annual event divided by total deposits), HSBC had the highest annual incident per $ billion of deposits (21.293) and ING Bank the lowest (one event, 0.085 per billion). In terms of complaints, the highest number recorded was 1,117 per month. Hoofnagle's study provides the first evidence of the extent of actual incidents at banks, and the first glimpse at how some banks suffer considerably more of these identity thefts than others.

There are several critical issues for financial institutions. It will be no surprise that the financial sector is hard hit by identity theft, as those firms are the most direct route for thieves attempting to steal customers' assets. Secondly, the free rider issue with respect to security of digital assets is starting to look more apparent. Because banks do not report their experiences, or costs of losses, consumers can't choose a bank based on how safe it is. There is the chance that the current US plans to overhaul the financial regulatory system will require more disclosures regarding online safety. Lastly, because the market itself is unable to protect the payment system, there will be industry initiatives, such as the Payment Card Industry Data Security Standard, to try to improve online safety for consumers. As will be seen later, although the PCI DSS goes a long way, its effectiveness is hampered by noncompliance among firms required to comply.

3.0 Research Methodology

This paper makes use of the case study method of field research to examine the risks to the banking and financial services industry and its customers from identity theft. This is an intrinsic case study (Stake, 1994). "Intrinsic casework regularly begins with cases prespecified." (p. 243) And that is the case with large-scale identity theft – the theft or data breach has already happened, and the researcher has that event, and similar ones, to use as a population. In looking at examples of large scale identity theft perpetrated against U.S. business organizations and/or their customers, the paper seeks to provide an avenue for an organization's management to understand its own issues and risks, with respect to the threat, and to address that with a well-conceived plan.

4.0 Discussion and Findings

4.1 The Evolution of Identity Theft

As Peretti (2009) notes, identity theft was a problem before the Internet existed. What's new, and what has changed this type of fraud, is the distribution/marketing system. The means to market products, especially digital products, that the Internet made possible for legitimate business has also been given to illegal businesses and organized crime. Criminals have found identity theft to be an easy way to steal, with little chance of prosecution. The discussion of carding forums in the literature review (Peretti 2009) reveals a number of large, international websites dedicated to the buying and selling of stolen identities, good and services necessary to carry out identity theft on a large scale. *The pervasiveness of the problem can be seen in three dimensions: (1) the estimated fraud costs of identity theft (U.S. numbers only); (2) the widespread attempts at stealing identities; and (3) costs to financial institutions.*

Javelin Research and Strategy has estimated via survey consumer fraud losses for the last three years:

Table 1. Estimated Costs of Identity Theft in the U.S.

Year	Fraud Losses	No. of cases of identity theft
2006	$49.3 billion	8.4 million
2007	$45 billion	8.1 million
2008	$48 billion	9.9 million

The table above only shows the amounts stolen. In most cases the consumer's liability will be limited to $50, leaving the merchant, bank, or card issuer to absorb the balance. Besides the actual amounts stolen, consumers will spend money on out of pocket expenses (copying, phone calls, etc.) to clear the matter, and it will take time to resolve the theft. Using 2006 data as an example, total losses were the $49.3 billion stolen, plus $4.9 billion in out-of-pocket expenses, plus $6.7 billion worth of time (Schreft, 2009) for a total $60.9 billion.

4.2 Methods of Identity Theft

There are many ways to steal an online identity but here the focus is on those methods that affect many consumers every incident. In order of increasing numbers of individuals affected by each incident of a specific type, the discussion begins with keylogger program, then to the phishing emails/phishing websites campaigns, and concludes with data breaches. Email attachments and music downloads. These are a popular way to install a keylogger program on many users' computers. A keylogger program records a user's keystrokes (which would include usernames, passwords, and the URL of the sites visited) and sends the data back to the thief. While many users have been victimized this way, on a per-incident number of victims, this method is likely less successful than phishing attacks.

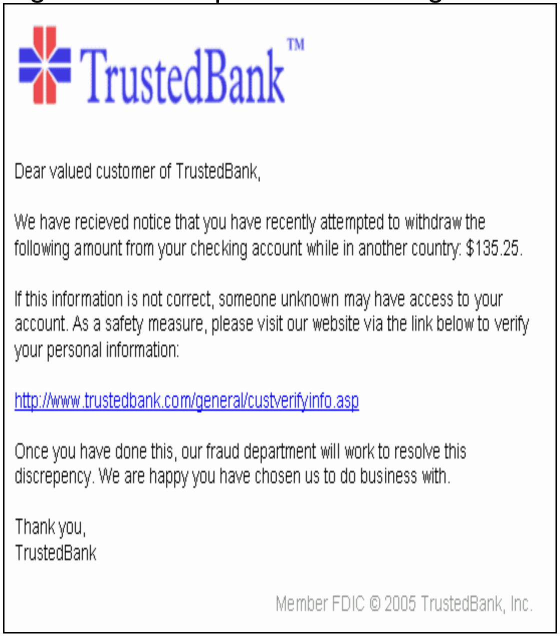
Website spoofing is a two-step process that takes advantage of well-known organizations' websites. First an organization is chosen that is likely to yield a large number of users. A phishing email will be spammed to thousands or millions of email accounts. Many phishing emails purport to be from a bank or financial services firm, with an announcement that there is a urgent problem with the user's account. Of course users not having such an account will disregard the message, but about five percent of recipients will fall for it (Synovate, 2007). Citing security concerns, or system upgrades, or questionable activity, the message (see Figure 1) will direct the user to click on a link inside the email to take them to a fake ("spoofed") website. When the user enters his or her username, password, and account number, the thief will have collected most or all of the needed identity elements to steal the user's identity, and the assets in the account at the organization whose website was spoofed.

Symantec, a producer of Internet security products, tracks the numbers of phishing emails it blocks. From January to July 2007, the service blocked over 12 million phishing emails daily (Schreft, 2009). Symantec reported that in April 2009, "One in 404.7 emails (0.25%) comprised some form of phishing attack." Symantec Corp., 2009b). The number of phishing websites has increased considerably since phishing websites kits became available. The Anti Phishing Working Group (APWG), an industry consortium, tracks the number of unique phishing websites reported to it. For the month of October 2008, there were 27,739 sites reported. Also increasing, the consortium reported, was "the number of crimeware-spreading sites infecting PCs with password-stealing crimeware (reaching) an all-time high of 31,173 in December 2008." (APWG, 2008). In its report for the first half of 2008, it noted that some 47,324 phishing attacks had been identified. It defines an attack as "…a phishing site that targets a specific brand or entity."

Data breaches, in which the records stored on an organization's computer system are inadvertently exposed or stolen, is another way identities are compromised by the thousand or millions. Data breaches are a way of harvesting a large number of identities from a single organization that is likely to have thousands or millions of records available to steal. The guilty parties may be insiders, business partners, or external parties. Conventional wisdom was that usually insiders were to blame, but Verizon's Data Breach Report (2009) shows that the majority of breaches are by external hackers exploiting a flaw in the security system. In the Verizon report, a number of the breaches were tied to organized crime.

Verizon (2009) reported that for the data breaches in investigated in 2008, 30% were in financial services firms. Retailer accounted for 31%, and the food & beverage industry was involved in another 14%. In 2008 alone, these 90 cases compromised 285 million records. Ninety-three percent of those records compromised were the result of just five breaches. The mean number of records compromised was 4.5 million; the median was 37,847 records. External parties (hackers) were responsible for 74% of these; business partners for 32% and insiders were involved in 20%. (Numbers sum to >100% due to the involvement of more than one group in an incident.)

Figure 1. Example of a Phishing Email



Dear valued customer of TrustedBank,

We have recieved notice that you have recently attempted to withdraw the following amount from your checking account while in another country: $135.25.

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

http://www.trustedbank.com/general/custverifyinfo.asp

Once you have done this, our fraud department will work to resolve this discrepency. We are happy you have chosen us to do business with.

Thank you,
TrustedBank

Member FDIC © 2005 TrustedBank, Inc.

Although there have been some large-scale breaches recently, The number of events and the scale do not appear to be slowing or shrinking. The seminal event for raising public awareness was probably the Choicepoint breach in 2005 (163,000 records) which California law required to be reported to affected consumers. DSW, Inc. suffered the loss of data on 1.4 million credit cards between November 2004 and February 2005. CardSystems Solutions Inc. lost data from 293,000 accounts in September 2004. The largest one to date (until 2009) was TJX Companies Inc., with a breach of 94 million accounts in Jan. 2007. In 2009, Heartland Payment Processors announced it had discovered software on its systems that read captured transaction data as it was being processed, and sent it to the thieves. Heartland processes 100 million transactions a month for some quarter-million merchants. Presently the extent of the damage is unknown.

Although the industry has produced a set of rules for members to follow, the resulting Payment Card Industry Data Security Standards (PCI DSS) is not entirely effective. The Verizon report (Verizon, 2009) noted large noncompliance with the standards. It noted "Over thee-quarters of organizations suffering payment card breaches within our caseload were found not compliant with PCI DSS or had never been audited." Of the 90 cases, 19% had been in compliance during the most recent assessment (41). Of the 12 requirements of PCI DSS, Verizon found that "the average compliance rate across victims in our caseload to be 20 percent…". Another issue for firms is reliance on antivirus software to safeguard their systems. Verizon noted that 40 percent of firms did not use this tool. Relatedly, the software ("sniffers") that thieves install on company computers to read transactions is not detected by antivirus software. The Heartland

Payment Processors data breach was caused by a sniffer. Heartland could not say how it got into their system, or how long it had been there.

4.3 Costs

Among the costs suffered by financial firms due to identity theft, one can count the following. Costs to reissue compromised debit/credit cards. An estimate of $10-$12 per card was provided for the Hannaford Brothers data breach. Some 4.2 million identities were compromised in March, 2008, with 1,800 fraudulent charges made. Lawsuits against PCI certifiers. In the fallout from the CardSystems failure, Merrick Bank is suing Savvis Inc. for $16 million, alleging negligence in certifying Merrick's processor, CardSystems, as being in compliance with PCI standards, only to be found in noncompliance after a breach. If the lawsuit succeeds, PCI certifiers will face a much riskier environment, with higher prices to compensate. Those prices will be passed on to firms needing their transaction processors certified. The average cost of a data breach in the US in 2008 was $6.7 million; the highest was $32 million. (Ponemon, 2008). On a cost per record basis, data breaches are costing $100 per record to resolve.

4.4 Loss of Customer Confidence

Hoofnagle's (Hoofnagle, 2008) research into bank's identity theft experiences may mean that customers will now demand that information from their financial institutions. As customers become aware of their bank's record with respect to protecting their identities, customer turnover ("churn") may increase at banks with the poorest records. Customers will likely leave a firm which has suffered either data breaches or website spoofing attacks. A 2005 study noted that the firms enjoying the highest customer trust with respect to maintaining customer trust were severely discounted following a severe spoofing attack (Ponemon, 2005).

4.5 Suggestions To Reduce The Risk

The following suggestions are offered as ways to implement a response to the threats discussed above.

1. Determine if your firm is in compliance with the Payment Card Industry Data Security Standards. If it is not, create a means of addressing the shortfalls.

2. Identify what types of personally identifiable information is kept. Consider your data retention plan, why the PII is collected, where it is stored, and who (employees and business partners) has access.

3. Develop a contingency plan. Create a phishing/data breach response team. Determine you're your probable response will be. Identify the best means to notify customers. Identify the best ways to pursue legal action.

4. Register your website with a security firm so that you will be notified of spoofing attempts. Identify website URLs close to your firm's URL. Who are the owners?

5. Consider planting bait records in the files.

6. Send an authorization code with transaction details to your customers so they can authenticate it. This is helpful in card not present transactions.

7. Consider offering identity theft protection to customers. This would be a real value-added service and offer a competitive edge.

8. Manage customers' changing of passwords. Email a confirmation each time a customer changes a password.

9. Tell customers about the phishing problem. Explain that you are taking steps to protect their sensitive information, but they must not be tricked into giving it away. Tell your customers about key logger programs. (This type of program is disguised inside downloads or in e-mail attachments. When it installs itself on a customer's PC, it will copy the keystrokes the user enters to visit particular websites, such a credit cards and online financial institutions. The program then sends the information out to the criminal.)

10. Encourage customers to report phishing attacks.

5.0 Conclusions

This paper has provided a summary of major issues facing the financial services industry regarding identity theft and the resulting issues needing to be addressed. Discussion of the major techniques for enabling identity theft, the scope of the problem, and some proposals for minimizing the risks to the industry were offered.

6.0 References

Anti-Phishing Working Group, 2008. *Phishing Activity Trends Report, Q1/2008.*

Anti-Phishing Working Group, 2009. *APWG releases Second Half 2008 Phishing Trends Report.* http://www.APWG Phishing Trends Activity Reports.

Hoofnagle, Chris. 2008. *Measuring Identity Theft at Top Banks (*Version 1.0) February 26, 2008. Berkeley Center for Law and Technology. Retrieved 8/18/2009 from www.finextra.com/finextra-downloads/newsdocs/hoofnagle.pdf

Javelin Research and Strategy. 2007. http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study.

Peretti, Kimberly Kiefer. 2009. "Data Breaches: What the Underground World of "Carding" Reveals." *Santa Clara Computer & High Tech Learning Journal.* Vol. 25, pp. 376-413.

Ponemon Institute LLC, 2005. *2005 Most Trusted Companies for Privacy Study.*

Ponemon Institute LLC, 2008. www. encryptionreports. com/download/Ponemon_ COB_2008_US_090201.pdf.

Schreft, Stacey L. 2007. "Risks of Identity Theft: Can the Market Protect the Payment System?" *Economic Review*, 4th Quarter, Vol. 92, Issue 4, pp. 5-40.

Stake**,** Robert E. Stake. 1994. Case Studies. *Handbook of Qualitative Research.* Norman K. Denzin and Yvonna S. Lincoln (Eds.). Chapter 14, pp. 236-247. Sage Publications. CA: Thousand Oaks

Symantec Corporation. 2009a. *Symantec Global Internet Security Threat Report: Trends for 2008.* Vol. XIV.

Symantec Corporation. 2009b. *April 2009 MessageLabs Intelligence Report.*

Synovate, 2007. *Federal Trade Commission – 2006 Identity Theft Survey Report*. http://www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Verizon Business. 2009. *2009 Data Breach Investigations Report.* http://www.verizonbusiness.com/resources/security/reports/2009_databreaches _rp.pdf