Identity Theft: A Pernicious and Costly Fraud*

Julia S. Cheney

December 2003

Summary: *On October 3, 2003, the Payment Cards Center of the Federal Reserve Bank of Philadelphia sponsored a workshop on identity theft to examine its growing impact on participants in our payments system. Avivah Litan, vice president and research director of financial services for Gartner Inc., led the workshop. The discussion began and this paper follows with a broad study of identity theft, at times compared with traditional payment fraud, and continues with an evaluation of its overall risk to consumers, merchants, and credit providers. The paper compares the incentives each such party has to address identity theft in concert with current market response to the crime. Finally, the paper concludes by posing several questions for further study. This paper supplements material from Litan's presentation with additional research on the crime of identity theft.*

* The views expressed here are not necessarily those of this Reserve Bank or of the Federal Reserve System.

FEDERAL RESERVE BANK OF PHILADELPHIA

Ten Independence Mall, Philadelphia, PA 19106-1574 • (215) 574-7220 • www.phil.frb.org

Introduction

In October 2003, the Payment Cards Center held a workshop to examine the growing problem of fraud associated with identity theft: the impact on consumers, merchants, and credit providers and the efforts being made by each party to reduce exposure to such fraudulent activity. Avivah Litan,[1] vice president and research director of financial services for Gartner Inc.,[2] led the workshop. She began the discussion by differentiating fraud associated with identity theft from the more traditional forms of payment fraud experienced by credit card providers and other lenders. Identity theft is in many ways a more pernicious action that can have long-term effects on consumers and significant financial impact on merchants and lenders. Since identity theft is a relatively new phenomenon, our understanding of it and its impact is still evolving. Nevertheless, as criminal behavior patterns are identified, early-stage prevention strategies are being developed. It is becoming increasingly evident that to prevent crimes associated with identity theft and to support victims of this fraud, ongoing and coordinated effort among the industry, policymakers, and consumer groups is necessary.

The comprehensive impact of identity theft is not yet fully understood, but recent studies highlighting the rapid growth and significant costs associated with the crime have spurred debate and a search for solutions. Early discussion around identity theft relied on anecdotal evidence largely reported by the popular press. Trade groups and government agencies[3] responded with

---

[1] Litan has written several articles, published by Gartner, Inc., on identity theft, including "Underreporting of Identity Theft Rewards the Thieves," 7/7/03; "Identity Theft Fraud Prevention Solutions Start to Proliferate," 7/7/03; "Reduce Identity Theft by Rectifying Too-Easy Credit Issuance," 9/4/03; and "Study Shows Financial Firms Need to Act Against Identity Fraud," 9/23/03. She has also been quoted by the Washington Post, American Banker, and Los Angeles Times, among others, on the topic of identity theft.

[2] Gartner Inc.'s web site, http://www.gartner.com, states "Gartner, Inc. is a research and advisory firm that helps more than 10,000 clients leverage technology to achieve business success. Gartner's businesses consist of Research, Consulting, Measurement, Events and Executive Programs. Founded in 1979, Gartner is headquartered in Stamford, Connecticut and has over 3,800 associates, including approximately 1,000 research analysts and consultants, in more than 75 locations worldwide. Fiscal 2002 revenue totaled $888 million."

[3] The Federal Reserve Bank of Boston has published a brochure titled "Identity Theft" and a video titled "Identity Theft: Protect Yourself" that list steps consumers can take to protect themselves against identity theft. This document can be found at www.bos.frb.org under the section on consumer information. The Federal Trade Commission has outlined consumer guidelines on the FTC's web site in a document titled

information guides attempting to alert consumers to the risks associated with identity theft and to offer suggestions as to how best to protect personally identifiable information from identity thieves. More recently, the Federal Trade Commission issued a report that attempts to quantify the costs to individuals and businesses. This report, titled "Identity Theft Survey Report" (hereafter, FTC Survey), estimates the cost of identity theft to individuals and businesses to be $3.8 billion and $32.9 billion, respectively.[4] In her remarks, Litan also cited a Gartner, Inc. study that provides another set of estimates on the frequency and severity of identity theft that confirmed the significant and rising costs associated with identity theft. Litan suggested that the release of such data highlights a need for market participants to re-calibrate the portfolio fraud risk assumed to be tied to the crime of identity theft and for policymakers and law enforcement agencies to continue to increase their focus on this significant and growing problem.

Motivated by the workshop discussion, this paper begins with a review of recent legislation defining identity theft as a crime and follows with Litan's further delineation of payment fraud and identity theft. The Internet's central role in facilitating the growth of fraud is analyzed in terms of its use by criminals as a means to access and then to fraudulently employ stolen personal data. The paper also reviews the scope and financial impact of identity theft and considers the respective market incentives to address the issue across affected parties, specifically, consumers, merchants, and credit providers. The paper concludes with Litan's review of current approaches being employed to mitigate and control identity theft and leaves several questions for further study. This paper supplements material from the workshop with

---

"ID Theft: When Bad Things Happen to Your Good Name." This report can be found at http://www3.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#risk.

[4] The Federal Trade Commission's *Identity Theft Survey Report* was released in September 2003 and is available at the Federal Trade Commission's web site at http://www.consumer.gov/idtheft. The FTC Survey characterizes three types of identity theft, including the following: "New Accounts and Other Frauds," "Misuse of Existing Credit Cards or Card Numbers," and "Misuse of Existing Non-Credit Card Accounts or Account Numbers." The cost to individuals and businesses referenced in this instance relate only to the category "New Accounts and Other Frauds."

additional research on identity theft and its significance in today's technologically driven credit markets.

The Legislative Codification of Identity Theft

The term "identity theft" was first codified in the Identity Theft and Assumption Deterrence Act of 1998.[5] This act makes it a "federal crime when someone knowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of federal law, or that constitutes a felony under any applicable state or local law." Additionally, the act defines a "means of identification" as "any name or number that may be used, alone, or in conjunction with any other information, to identify a specific individual." Identifying information is noted to be, among other things, a name, SSN, date of birth, driver's license or passport number, employer or taxpayer identification number, or telecommunication identifying information or access device. Finally, the law directs the Federal Trade Commission (FTC) to establish a central complaint system to receive and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

The Definitional Dilemma

The industry and the press often apply the term "identity theft" to various forms of fraudulent activity, including payment fraud. In Litan's view, a tightening of the definition is necessary to effectively motivate the exchange of relevant information and to promote the policy dialogue she believes is needed to combat this growing criminal activity.

Litan defined payment fraud as the misuse of stolen customer account information for financial gain. The most common form of payment fraud is credit card fraud in which stolen

[5] The Identity Theft Assumption and Deterrence Act of 1998 can be found on the Federal Trade Commission's web site at www.ftc.gov/os/statutes/itada/itadact.htm.

credit card account data, including, most notably, the credit card number, are employed by criminals to obtain cash or goods using the victim's credit accounts. The victim typically identifies such fraud when spotting inaccuracies in monthly statement information or as a result of notification by the financial service provider.[6] According to the FTC Survey, 39 percent of victims detected credit card fraud in less than one week, and only 8 percent of victims took six months or more to make the discovery. This relatively rapid identification allows for prompt remedial action that generally includes canceling the card to prevent further criminal misuse. The important distinction for the purposes of this discussion is that the more common forms of credit card fraud typically involve only a single account and perhaps a few fraudulent transactions before the fraud is recognized and the card cancelled. As we will see in the case of fraud associated with identity theft, the situation is far more complex. Fraud losses associated with identity theft can be significant, involve multiple accounts, remain undetected for much a longer period, and ultimately result in costly and time-consuming efforts to re-establish the victim's credit standing.

Turning to fraud associated with identity theft, Litan defined identity theft as the stealing of personally identifiable private information and the use of such data to impersonate an individual in order to establish original credit or hide criminal activities. (This discussion focuses only on identity theft perpetrated for the former purpose.) Again, the distinction made here is that fraud associated with identity theft relates to the establishment of new accounts as opposed to the theft of existing account information, as in the case of traditional payment fraud. Further, Litan made the point that fraud associated with identity theft may not even include a human victim. Particularly savvy criminals are able to create synthetic identities that are then used to establish new credit accounts. If there is a human victim, identity thieves tie the new credit accounts, such as cellular phone service, credit cards, and short-term loans, to address and contact information

[6] Financial services companies and technology providers have developed sophisticated fraud-detection systems that monitor credit card use and flag unusual account behavior. These allow pre-emptive action,

different from that of the victim. Thus, the thief is able to successfully transfer the point of contact with creditors and, in this way, hide the theft from the victim. Identity theft is generally discovered by the victim either when the fraudulent account activity registers on the credit report (and, atypically, the credit report is reviewed by the individual) or more commonly, when the creditors attempt to collect on delinquent payments. Litan asserted that most damage is done to these accounts in the first three months, and unfortunately, victims typically do not recognize the fraud until much later. According to the FTC Survey, and in contrast to payment fraud, only 17 percent of victims detected identity theft in less than one week, but notably, 24 percent of victims took six months or more to make the discovery.

During the longer discovery period associated with identity theft, the fraudulently created accounts are systematically exploited, leaving the unsuspecting creditors and merchants with often sizable losses. The industry uses the term "bust-out fraud" to describe this phenomenon, since criminals will often take considerable time to build multiple account relationships before "busting-out." As will be discussed later in greater detail, the FTC Survey indicated that when compared with traditional payment fraud, identity theft represented more than two times the cost to businesses and more than three times the cost to victims – all of which suggests the problem is significant and lacking many of the detection tools and preventative measures that have been developed to combat traditional payment fraud.

Methods Used to Steal Private Identification and Account Data

The perpetration of payment fraud and identity theft begins with the stealing of individually identifiable private data accessed by thieves using various means, including the Internet. Litan noted that it has proved relatively easy for hackers to access private and sensitive information stored on some servers via the Internet. Further, there seems to be a developing international sub-culture of technically advanced criminal elements sharing pieces of stolen

---

such as calling customers to confirm purchase activity and address possible fraudulent account activity.

personal information, including, most prominently, credit card data, over the Internet. These criminal gangs are loosely organized and use the stolen data to launch concerted fraud attacks. Litan stressed that even though international fraud sources currently appear to be highly concentrated, with the industry identifying Indonesia, Russia, and Nigeria as some of the particularly problematic areas, they are also very mobile and difficult to pin down, making detection and prosecution especially difficult.

At the same time, Litan emphasized that fraud, and identity theft in particular, is not necessarily a high-tech crime. A review of data provided by victims who believed they knew the method used to steal their personal information showed that simple techniques were common, including mail intercepts, lost/stolen wallets or identification cards, and subterfuge by family, friend, neighbor, or co-worker. Although the FTC Survey indicated that almost half of victims did not know how their personal data had been stolen, a significant 26 percent[7] knew the identity of the person who stole their personal information, and it was often family, friends, or co-workers.

The Internet Effect

In addition to being a means for stealing personal identification data, the Internet also represents a preferred platform for the perpetration of identity theft as well as traditional payment fraud. For the identity thief, the anonymous transactional environment characterized by Internet commerce provides a real advantage. The absence of direct physical contact between transacting parties makes it easier to use stolen personal data to impersonate an individual. As a simple illustration, a 50-year-old man could present himself as a 25-year-old woman without detection in the anonymous online world, whereas such deception would be highly unlikely to occur in the face-to-face, brick-and-mortar sales environment. This "cover of anonymity" is relatively unique

to the Internet[8] and acts to protect criminals from identification, creating special challenges for law enforcement agencies attempting to arrest and prosecute the perpetrators.

At the same time, consumers' use of the Internet to effect commercial transactions continues to grow at a rapid pace. Banks and retailers are also increasing their use of the Internet as an alternative channel for the solicitation of new credit accounts and for the sale of products and services. While fraud is reasonably well managed in the mature (flat growth) brick-and-mortar sales environment, it presents greater challenges in the growing commercial online channel. In fact, Litan noted that traditional payment fraud in the brick-and-mortar arena is declining; she estimated that it is currently less than 0.06 percent of sales. Alternatively, she stated that in the online world, associated fraud losses are much higher as a percentage of sales, and notably, these total losses are growing overall as a result of significant increases in total online sales. According to the U.S. Department of Commerce, Internet sales grew at a rate of 25 percent in 2002, reaching $43.5 billion.[9] Supporting Litan's view, the results of an online merchant survey released by CyberSource[10] indicated that credit card payment fraud across participating merchants reached 1.7 percent of online sales in 2003, over 28 times higher than in the brick-and-mortar world. All of which supports that payment fraud in the brick-and-mortar environment is a relatively mature

---

[7] Includes the Federal Trade Commission's three types of identity theft "New Accounts and Other Frauds," "Misuse of Existing Credit Cards or Card Numbers," and "Misuse of Existing Non-Credit Card Accounts or Account Numbers."

[8] Also, to a lesser extent, catalogue sales via telephone and direct mail offers are conducted under the same "cover of anonymity."

[9] U.S. Department of Commerce: Commerce News "Retail e-Commerce Sales in Second Quarter 2003 Were $12.5 Billion, up 27.8 Percent from Second Quarter 2002, Census Bureau Reports"

[10] CyberSource Corporation, "*Online Fraud Report – Credit Card Fraud Trends and Merchants' Response"* – 2004 Edition. The focus areas of this report include the following: online fraud's impact on business, merchants' efforts to manage fraud, and plans to combat online fraud in the future. The report can be obtained by contacting the company or through its web site. The survey methodology as described by CyberSource is as follows: "Merchants who participated in this survey reflect a blend of small-, medium-, and large-sized businesses based in North America. They represent companies in their first year of online sales to the largest e-retailers in the world. The mix of merchants (by size of online revenues) who participated in 2003 was nearly identical to those who participated in 2002. Predictably, however, participating merchants had more years of experience selling online in 2003. The survey was conducted via an online questionnaire at the Mindwave Research website. Three hundred thirty-three merchants completed the survey between October 14th and October 21st, 2003. All participants were either responsible for or influenced decisions regarding risk management in their companies."

phenomenon that is reasonably well managed by credit providers when compared with the newer and fast-growing Internet world of online transactions.

To summarize, the Internet is an important and growing commercial channel that, because of the inherent transactional anonymity, embodies significant systemic risk for fraudulent activity.

A particular challenge in the Internet transactional environment is the issue of customer authentication. Authentication, a critical element in the credit card authorization process, implies that the merchant has obtained a piece of verifiable private information, in addition to data available on the card itself, to further validate the identity of the individual making the purchase. Face-to-face credit card transactions typically present a situation where the card is present, and therefore, the merchant is able to obtain, relatively easily, additional information to "authenticate" the individual making the transaction. In the case of brick-and-mortar sales, for example, the sales person will cross-check the signature on the back of the credit instrument to that written by the customer, in person, on the store receipt. If there remains some doubt, the sales person can request additional forms of identification, including photo identification, and so forth. On the other hand, for commercial transactions that take place over the Internet (or via telephone), the card is, by definition, not present, and authentication of the buyer, using today's technology, is far more difficult.[11] Under bank card association rules, such transactions are placed in the "unauthenticated" category – unless the merchant has adopted the relatively new Verified by Visa program[12] – because the merchant is unable to obtain further verifiable data to confirm the customer's identity. The Visa and MasterCard fraud liability rules are central to the distinction between authenticated and unauthenticated transactions. According to these rules, the credit

[11] In the telephone catalogue sales environment, merchants can use the catalogue reference code printed on the mail order solicitation as a form of authentication. This allows at least some level of assurance that the person ordering the merchandise is the one to whom the merchant directed the solicitation. In the Internet sales arena, buyers come to the merchants' site with complete anonymity.

[12] Verified by Visa represents a security protocol introduced by Visa in 2001. Merchants who implement Verified by Visa and request a PIN from a cardholder, which is then validated by participating card issuers, are not liable for fraud; rather, the card issuer is. MasterCard has a similar program called MasterCard

issuer assumes fraud risk associated with authenticated transactions while the merchant assumes fraud risk associated with unauthenticated transactions.

While merchants await the development and full deployment of Internet-capable and widespread industry-endorsed authentication technology like Verified by Visa, they are testing and implementing a variety of tools themselves in an effort to limit losses associated with unauthenticated online transactions. The previously referenced CyberSource survey indicated that merchants were increasing efforts in 2003 to combat online fraud through the implementation of various preventative measures. As examples, the following tools were identified in order of current adoption rates: Address Verification Service (AVS), manual review, internally built business rules/decision rules, card verification number (CVN), commercial fraud screen/risk scoring service, Verified by Visa, commercial fraud screening/risk scoring software, and MasterCard SecureCode. Notably, the CyberSource survey estimated that merchants' use of manual review has increased significantly – from 52 percent in 2002 to 65 percent in 2003. Manual review can be a time-intensive and costly process involving, many times, not only further attention by the merchant's staff but also additional contact with the customer; therefore, manual review, although helpful in fraud reduction, adds to the indirect costs of fraud for online merchants. While the merchant community is taking important first steps toward preventing online fraud, in Litan's view, until such time as authentication technology is ubiquitous and has buy-in by not only merchants but also credit card providers and consumers, none of these currently available tools will be able to significantly reduce fraud losses across a wide base of merchants, especially since only the largest merchants have the resources required to implement effective fraud prevention solutions and processes.

SecureCode, but this program only reverses liability from merchants to card issuers when the consumer actually provides a PIN, not just when a merchant asks for a PIN.

The Pattern of Identity Theft

Once thieves have stolen personal data and set out to commit identity theft, as opposed to traditional payment fraud, they tend to follow a typical pattern to build validity into a stolen identity. Initially, the thief establishes an address that is different from the one used by the victim and, obviously, accessible by the thief. Litan noted that criminals often acquire a cellular phone and use this account as the first step toward building data in a credit bureau file tied to the new address. Cell phone service can be contracted on an instant-approval basis in a card-not-present environment and, therefore, offers a low probability of detection. At the same time, the thief can determine whether the stolen identity information will pass the "usability test." The next step to building credit is to establish a bank account with a small amount of money, say about $250, to continue to deepen the credit file with positive data. Then, the thief will apply for credit cards and increase the associated lines in a concerted approach to maximize the "take." Sometimes, a thief will establish other credit under the falsified identity, such as short-term bank loans or even secured auto loans. Finally, as previously described, the thieves "bust-out" by fully utilizing the lines and then abandoning the accounts, leaving the victim, merchants, and credit providers with the loss and the task of sorting out the fraudulent activity and associated liabilities.

Scope of Identity Theft

As the criminal pattern of identity theft has emerged, it has raised questions regarding the impact of identity theft on business and on consumers and, importantly, led to the Federal Trade Commission Survey Report and Gartner's independent analysis of this issue. The research findings recently released by these two organizations suggest the size of the identity theft problem is much larger than was assumed using the earlier proxy: the number of registered complaints in the FTC Consumer Sentinel complaint system. In fact, the number of identity theft complaints

recorded in this system was only slightly more than 160,000 in 2002.[13] In contrast, the newer FTC Survey and Gartner's identity theft research produced numbers that are significantly higher: 3.2 million and 7.0 million, respectively. These studies cover roughly the same period: mid-2002 to mid-2003. Litan stated that despite the scale differences represented in the FTC and Gartner data sets, both studies forcefully demonstrate the apparent past under-estimation of identity theft.[14] Litan further noted that based on Gartner's estimates, identity theft crimes increased 79 percent from 2002 to 2003. Importantly, Litan noted that identity theft may be an even greater problem than these studies suggest. According to a recent report by San Diego-based ID Analytics,[15] a significant amount of identity theft may be missed because it results from synthetically created identities where there is no real consumer victim and, therefore, no one to report the crime.

Financial Impact of Identity Theft

The FTC Survey details the financial impact of identity theft, both in terms of opportunity cost and losses to businesses and individuals. Opportunity cost is defined as the forgone work hours or leisure time re-allocated to resolving errors related to identity theft in the victim's credit file. The chart below shows the results of the FTC Survey in terms of dollar losses

[13] The Federal Trade Commission reviewed complaints filed in the Sentinel complaint system in its report titled "National and State Trends in Fraud and Identity Theft: January 2002 – December 2002" p. 3. This report can be found at http://www.consumer.gov/sentinel/pubs/Top10Fraud_2002.pdf

[14] GAO testimony on Identify Fraud: Prevalence and Links to Alien Illegal Activities, June 25, 2002, before the Subcommittee on Crime, Terrorism, and Homeland Security and before the Subcommittee on Immigration, Border Security, and Claims, Committee on the Judiciary, House of Representatives. This June 2002 testimony also suggests that identity theft may be a larger problem than had been previously assumed given available documentation. The testimony also addresses the broader implications of identity theft in regard to immigration, terrorism, and narcotics trafficking.

[15] A September 23, 2003 ID Analytics press release posted on its web site, www.idanalytics.com, discussed the "National Report on Identity Fraud," saying that "the year-long research project leading up to this report analyzed more than 200 million records, including valid and fraudulent consumer applications for credit, debit and new accounts, together with the largest collection of cross industry known frauds to date." The press release also states that "an overall key finding is that a surprising portion of the identity fraud perpetrated against businesses is actually without a consumer victim because the fraudulent identity is fabricated. In fact, 88.4 percent of identity frauds discovered through the research were not originally reported as such by businesses due to the criminals' ability to obfuscate traces of the crime."

to businesses and victims as well as average resolution time for the victim. The data show the disparity in financial loss and time to both businesses and victims of identity theft versus "misuse of existing accounts," or traditional payment fraud. Most notably, on an aggregate basis, identity theft losses to businesses are over two times and losses to victims are over three times that associated with traditional payment fraud.

	IDENTITY THEFT	MISUSE OF EXISTING ACCOUNTS*
Loss to Businesses, incl. Financial Institutions	$32.9 Billion	$14.0 Billion
Average Per Victim	$10,200	$2,100
Loss to Victims	$3.8 Billion	$1.1 Billion
Average Per Victim	$1,180	$160
Hours Spent by Victim to Resolve	60 Hours	15 Hours

Source: FTC - Identity Theft Survey Report: pp. 6-7
* Includes both credit card and non-credit card existing accounts

The Real Cost of Identity Theft to Consumers, Merchants, and Credit Providers

The financial impact of identity theft and traditional payment fraud, as described above, is significant on its own, but systemic and other indirect fraud-related costs are also borne by consumers, merchants, and credit providers. Consideration of such costs on an integrated basis adds clarity to the complex nature of the market incentives these parties face in addressing the issue. In general, Litan suggested that both consumers and merchants are especially motivated to reduce fraud associated with identity theft, but they must rely on credit providers, a more centralized group, to drive the implementation of improved fraud protection strategies or to develop endorsed authentication technology or both. In Litan's view, an important policy

question is whether industry solutions alone will be enough or will new initiatives be required to deal with this issue.

Consumers expect to have limited liability exposure related to financial fraud regardless of whether it is payment fraud or the more intrusive identity theft. At the same time, credit providers are motivated to provide such coverage to encourage these same consumers to apply for loans and, particularly as it relates to credit cards, to use the credit product. With respect to identity theft, consumers' direct financial liability is ultimately limited, but in reality, victims face significantly higher overall financial costs. These costs take several forms, including actual dollar loss (clean-up cost), credit score deterioration, forgone investment, and sacrificed leisure time. Litan suggested that these additional costs are a result of the presumption that the identity theft victim is "guilty until proven innocent" (i.e., the credit provider does not immediately assume fraud) as opposed to, for example, the victim of payment fraud, who is considered "innocent until proven guilty" (i.e., the credit provider immediately assumes fraud). In terms of identity theft, the requirement to prove fraud leads to a delay before action can be taken to control the associated fraud exposure. This delay is crucial because it provides more time for thieves to continue the fraud associated with the stolen identity and, hence, increases the total losses realized by all parties. This lag in recognition exacerbates the problem of detection, containment, and prevention of identity theft that, by its very nature, already proves to be an extremely complex crime.

The Internet and the absence of ubiquitous authentication technology play a crucial role in the level of merchants' assumed risk for fraud. Specifically, Internet transactions, catalogue sales via telephone, and mail order transactions are card-not-present and typically unauthenticated transactions. As such, card association rules dictate any associated fraud loss be charged back to the merchant's account (unless the merchant has implemented Verified by Visa and requested a Verified by Visa password from the consumer). In contrast, in the brick-and-mortar world of card-present, or authenticated, transactions, card association rules tie associated fraud losses to

the credit issuer. Again, because the Internet offers the cover of anonymity, it is a preferred channel for the perpetration of fraud, and as sales via this channel continue to climb, the fraud risk to merchants is growing disproportionately. Litan also noted that this exposure is skewed toward merchants in riskier product categories. But many of the larger, more sophisticated Internet merchants have invested in proprietary fraud detection technologies in an attempt to mitigate the risk, and they have had some relative degree of success.

In addition to the direct costs of fraud, Litan noted that merchants also assume indirect costs for these unauthenticated transactions, over and above those specific to non-payment risk. Litan estimated that merchants are charged 65 percent more in bank interchange fees for online transactions. Further, Litan estimated that merchants turn away 2 percent of valid transactions because they look suspicious. Notably, in an effort to reduce internationally originated fraud, Litan estimated that only 61 percent of merchants currently sell overseas and that 10 percent will stop doing so each year through 2006. Overall, she estimated that, on average, merchants are forgoing up to 10 percent in additional revenue potential via this channel. Internet merchants' fraud-related costs are high, and when those costs are combined with growing consumer fears of identity theft and, generally, of transacting on the Internet, a strong argument can be made that identity theft may threaten the growth of e-commerce overall.

From the perspective of the credit card issuer, fraud losses resulting from identity theft are dealt with the same as any other fraud losses; they are charged to the income statement when realized. As noted in the FTC Survey and Gartner's analysis, these losses are significant and growing. The ID Analytics study and its estimate of substantial synthetic identity fraud suggest the problem is even greater than the industry recognizes. Identity theft associated with synthetic identities is generally not captured as fraud, and losses are typically charged to the loan loss reserve. In these instances, there is no notification of fraud from a victim, and arrests that might be tied to the fraud are rarely made, making it difficult for creditors to confirm that the fraud has occurred. Industry sources note that a rash of returned payment checks or ACH credits are often

the only signals that a synthetic identity fraud has been perpetrated and too often these signals come too late. All of these factors are focusing industry attention on the problem.

In terms of traditional payment fraud, the credit card industry has done a good job of managing and containing payment fraud in the card-present environment, but it has had far less success in stemming fraud in the card-not-present environment. Litan suggested this is, in part, because the charge-back rules reduce the industry's incentives to do so. However, this could change if Verified by Visa gains mass adoption by consumers, giving card issuers a direct incentive to combat online payment fraud, as they absorb the charge-back and fraud costs under the Verified by Visa program. Absent compelling market incentives for the card industry, the open question is how will ubiquitous online authentication technology, crucial to the establishment of e-commerce as a channel of choice for both merchants and consumers, be developed?

Some industry thinkers recognize that their businesses' success to date has been due, in large measure, to their having created a safe and flexible payments environment that consumers and merchants trust. Any erosion of this trust could have serious implications for the industry and threaten the positive gains made in their business models and the evolving electronic payments system. In addition to their direct costs, credit providers experience the downstream effects of the costs to consumers and merchants in the form of reduced confidence in electronic payments and forgone revenue.

At the end of the day, any solution to identity theft must consider the costs discussed herein and needs to promote a balancing of incentives among consumers, merchants, and credit providers.

The Fight Against Identity Theft

Litan outlined current market responses to identity theft as efforts that fall into one of the three following categories: industry initiatives, consumer prevention, and government action.

Industry initiatives to date have been concentrated in developing authentication tools around the application process and, on the back end, instituting better data-sharing practices and streamlining consumer reporting requirements as it pertains to identity theft. Consumer prevention relates to consumer actions that can be taken to safeguard personal data from theft and reduce the impact of fraud. Governmental action, probably the broadest category, includes both regulatory and legislative initiatives as well as law enforcement and penalty determination.

In terms of industry initiatives, Litan reviewed three types of applications that have been brought to market in an effort to reduce the incidence of identity theft by addressing the authentication of individuals during the credit application process, i.e., application fraud. The first is single-source authentication, which can be either the issuance of an identifying PIN or code to the customer or the use of "out-of-wallet" data to further verify the customer's identity. Litan noted that the risk associated with an identifying PIN or code is that the thief also often steals this piece of data. Out-of-wallet databases use credit bureau data and specifically include information about the customer that typically cannot be discovered by stealing a person's wallet, for example, the type of student loans the person is holding. Credit providers can use such databases to ask customers more obscure questions on their credit applications that only they should know. The difficulty, Litan noted, is that these questions are often obtuse and difficult to answer even for the valid individual. Moreover, if, indeed, the thief has stolen this consumer's credit report, the thief will probably answer such obscure questions better than the true customer.

The second application type, multiple-source data validation, cross references the self-provided customer data on the credit application with consumer databases, including driver's license numbers, white pages, yellow pages, zip code, social security number ranges, and so forth, and confirms the consumer's application responses are correct. Again, in this case, Litan noted that if the thief has gained access to the victim's credit report, he will have all the correct data, and this type of authentication program will not detect the fraud. Further, the check of

application data against the multiple-source authentication database may not be real time and, therefore, presents a window of opportunity for fraudulent activity even in the case of a red flag.

The authentication tool that Litan believed best able to prevent identity theft is cross-industry pattern recognition because it works to predict identity theft before it happens. This tool brings together tracking data across affected industries, following thieves as they attempt to establish credit via a typical cross-industry pattern (cell phone service to bank accounts to credit card accounts to short-term loans). Litan argued that taking a cross-industry perspective will better allow the entire credit market to identify fraudulent patterns of behavior that holistically are recognizable but individually are not. Litan also stressed that using multiple tools or a layered approach to fraud detection and identity theft prevention is the preferred strategy and noted that, already, many banks are taking this approach by implementing a combination of the available tools and by leveraging a mix of internal databases, external databases, and manual checks.

In addition to application-based authentication efforts, the payment cards and banking industries have also begun working on an organized and more coordinated basis to establish a single point of contact for consumers to report identity theft. Increasing the reporting efficiency will reduce the financial impact and resolution time experienced by the customer and indeed by all affected parties. Two notable initiatives include the fraud alert system provided through the credit reporting agencies and, more recently, the proposal for an Identity Theft Assistance Center by the Financial Services Roundtable and BITS.[16] The fraud alert process allows a consumer to

[16] The Financial Services Roundtable's web site can be found at www.fsround.org. It describes BITS and their relationship as "BITS, The Technology Group for The Financial Services Roundtable, was formed by the CEOs of the largest bank-holding institutions in the United States as the strategic "brain trust" for the financial services industry in the e-commerce arena. BITS' activities are driven by the CEOs and their appointees–CTOs, CIOs, Vice Chairmen and Executive Vice Presidents–who make up the BITS Advisory Group and BITS Council. These leaders identify the issues, develop strategic recommendations and implement the CEOs' decisions. BITS also facilitates cooperation between the financial services industry and other sectors of the nation's critical infrastructure, government organizations, technology providers and third-party service providers." BITS' web site, www.bitsinfo.org, defines the organization as "a nonprofit industry consortium of the 100 largest financial institutions in the United States. Serving as the strategic "brain trust" for the industry, BITS focuses on issues related to e-commerce, payments and emerging technologies. Created in 1996 by industry leaders, BITS acts quickly to address problems and galvanize the industry to advance the interests of its members. BITS' activities are driven by the CEOs and their

place a single call to one of the top three credit bureaus and to have an alert put on his or her credit file at each of the three. In this manner, the alert process is centralized, more immediate, and less time consuming for the victim. The fraud alert also pre-establishes a credit approval process with the victim, requiring direct approval on all new credit applications tied to the consumer's credit record, for example, via a telephone call to a pre-specified phone number. Separately, on October 28, 2003, several financial services companies along with the Financial Services Roundtable and BITS announced the creation of the Identity Theft Assistance Center. This Center will act as a one-stop shop to allow identity theft victims to report the crime once and have this Center, at no charge to victims, handle the notification to credit providers at which the victim believes fraud might have occurred. The Identity Theft Assistance Center should be operational by the second quarter of 2004. [17]

Litan's discussion of consumer protection emphasized that individual consumers can employ simple practices to safeguard personal data and thereby reduce their exposure to identity theft. Litan specifically suggested that consumers keep personal data such as SSN and bank account numbers in a safe environment at all times, shred such documents prior to disposal, and provide personal data only with a clear understanding regarding the validity of a request.[18] To detect fraud as soon as possible, consumers must maintain attentive online monitoring of account activity and regular checking of credit report data. Further, Litan noted that victim assistance groups are a useful resource for consumers on the topic of identity theft, and she specifically

---

appointees—CIOs, CTOs, Vice Chairmen and Executive Vice Presidents—who make up the BITS Executive Committee, BITS Advisory Group and BITS Council. These leaders identify issues, develop strategic recommendations and implement the CEOs' decisions. Today BITS' top issues include cybersecurity, fraud reduction, identity theft, IT outsourcing, operational risk management and payments strategies."

[17] Press release, "New Center to Assist Victims of Identity Theft and Reduce Fraud," Financial Services Roundtable, October, 23, 2003. This press release can be found on the BITS web site at http://www.bitsinfo.org/nr.html

[18] Additional consumer guidelines are available on the FTC web site and are outlined in an FTC document titled "*ID Theft: When Bad Things Happen to Your Good Name,*" found at: http://www3.ftc.gov/bcp/conline/pubs/credit/idtheft.htm#risk

mentioned the Identity Theft Resource Center[19] as a leading consumer group on this topic. Finally, Litan made the point that such consumer groups are one way for consumers to organize and to speak with a centralized consumer "voice" on the topic of identity theft.

Government action, the third element outlined by Litan, has most recently been highlighted by efforts in the House of Representatives and the Senate to pass legislation to amend the Fair Credit Reporting Act (FCRA). FCRA, enacted in 1970, established obligations for credit bureaus, users of credit reports, and organizations that provide information to credit bureaus. Further, FCRA made the Federal Trade Commission the principal enforcer of these regulations.[20] On December 4, 2003, the FCRA amendment, the Fair and Accurate Credit Transactions Act of 2003 (FACT), was signed into law by the President of the United States.

For the purposes of this paper, following is a general review of the more relevant provisions related to identity theft that are included in FACT. The amendment will extend, permanently, state law preemptions and ensure a national standard as it relates to FCRA consumer protection provisions but not, as it happens, on a broad basis to identity theft prevention.[21] Only state law in conflict with FACT's identity theft provisions would be preempted. Still, this provision is important because it provides centralized and uniform management, in the form of federal legislation, as it relates to the use and protection of consumer financial information. The November 21, 2003 press release, "Conferees Reach Agreement on Landmark Identity Theft Legislation," by the House Committee on Financial Services,[22] outlined specific obligations for financial institutions to address identity theft, including the following: "requiring creditors to take certain precautions before extending credit to consumers who have

[19] The Identity Theft Resource Center is led by Executive Director Linda Foley and can be contacted through its web site www.idtheftcenter.org.
[20] Robert M. Hunt, "The Development and Regulation of Consumer Credit Reporting in America," Federal Reserve Bank of Philadelphia, Working Paper 02-21, pp. 16-17.
[21] Oscar Marquis, "Who Can Be Held Liable for Identity Theft?" American Banker, November, 18, 2003.
[22] The press release by the House Committee on Financial Services, "Conferees Reach Agreement on Landmark Identity Theft Legislation," dated November 21, 2003, can be found at: http://financialservices.house.gov/news.asp

placed 'fraud alerts' in their files; prohibiting merchants from printing more than the last five digits of a payment card on an electronic receipt; requiring banks to develop policies and procedures to identify potential instances of identity theft; requiring financial institutions to reconcile potentially fraudulent consumer address information; and requiring lenders to disclose their contact information on consumer reports." Additionally, the amendment provides for individuals to request and receive a free copy of their credit report every year from each of the three national credit bureaus, for consumers to place "fraud alerts" in their credit reports, and for consumers to block information related to identity theft from being reported to and by credit bureaus. Further, the amendment will result in identity theft victims' being provided with a summary of their rights. This legislation is an important step in establishing policy specific to the crime of identity theft, generally making it easier for consumers to access and monitor their credit report data and providing an added level of control over the sharing of such data when identity theft is suspected. Alternatively, it is still unclear whether such legislation will act as an effective criminal deterrent and motivate stakeholders sufficiently to curb identity theft's impact on our society and its payments system.

Conclusion

Identity theft is an escalating and significant fraud problem that not only is acknowledged by consumers, merchants, and credit providers but also has gained the attention of the regulatory and policymaking communities. Consumers are the most materially motivated to protect their identities, but because of this group's incumbent decentralization, they find it difficult to affect policy and practices sufficiently to limit their overall exposure. Merchants are a similarly decentralized community, and they depend on payment providers to endorse and employ appropriate identity authentication technology. Credit providers, credit reporting agencies, and processors have the data to best empower consumers with authentication tools and other means to safely manage their personal data and, in the unfortunate case of fraud, to mitigate the effect of

identity theft. Importantly, in the search for a solution to identity theft and like so many other aspects of network economies, balancing incentives among consumers, merchants, and credit providers is required to produce the best equilibrium.[23]

Progress is being made in the fight against identity theft, but in Litan's mind, a number of questions remain:

- Will growing fears about identity theft reduce consumer confidence in using electronic payments?
- Will lack of authentication affect consumer confidence in the Internet?
- Will lack of authentication technology lead to alternative online payment products?
- Does the payments system recognize identity theft early enough in the criminal process to successfully limit risk?
- What is the role of merchants in combating identity theft?
- What role can law enforcement agencies play in deterring this criminal activity?
- How can the burden of proof be shifted away from identity theft victims?
- Are additional regulatory or legislative initiatives required to better align the market incentives necessary to resolve these challenges?

In conclusion, this paper is intended to support the growing number of industry and public policy experts focusing attention on these questions. The analytical studies noted in the paper serve as first steps in better understanding the issues, but additional research and dialogue will clearly be required to develop appropriate solutions. At the end of the day, the costs to society and threats to efficiency of the payment system should be seen as critical factors to motivate these efforts.

[23] For an analysis of network economies, see Robert M. Hunt, "An Introduction to the Economics of Payment Card Networks," Working Paper 03-10, Federal Reserve Bank of Philadelphia.