Risks of Identity Theft: Can the Market Protect the Payment System?

By Stacey L. Schreft

Imagine sitting at a computer and with a few keystrokes having the personal information of person after person appear on the monitor: names, addresses, Social Security numbers, debit card account numbers and PINs, bank account numbers and passwords, mother's maiden name, and more. This happens every day, and the information is for sale in electronic markets. Buyers can use the information to commit fraud on existing financial accounts or on accounts opened with the information. This is the face of identity theft.

Identity theft has been a feature of financial markets for as long as alternatives have existed to cash transactions. Until recently, it occurred on a small scale, involving, for example, the theft of personal checks and the forging of the account holder's signature to cash them. That type of identity theft posed a risk to the individual consumer, and the risk was relatively small: Access to the consumer's personal checks did not offer access to all of the consumer's financial accounts.

Such individualized acts of identity theft still occur, but more often identity theft occurs on a larger scale. Data breaches typically involve the apparent loss or acknowledged theft of the personal identifying information of thousands—or millions—of people. This poses a risk to

Stacey L. Schreft is a vice president and economist at the Federal Reserve Bank of Kansas City. Danielle White, a research assistant at the bank, helped prepare the article. This article is on the bank's website at ***www.KansasCityFed.org****.*

the individual but also to the integrity and efficiency of the payment system—the policies, procedures, and technology that transfer information for authenticating and settling payments among participants. Identity theft can cause a loss of confidence in the security of certain payment methods and an unwillingness to use them. Markets can cease operating or switch to less efficient payment methods. Either represents a loss of efficiency for the economy.

This article looks at the nature of identity theft today and the factors driving its growth and explores whether markets are able to limit its risk to the payment system. Section I explains what identity theft is. Section II discusses the magnitude of the problem. Section III describes the factors behind the recent growth in identity theft. Section IV considers the risks identity theft poses to the payment system because markets provide too little protection for personal identifying information.

I. WHAT IS IDENTITY THEFT?

There is disagreement about how to define "identity theft." Commonly used definitions differ in the range of acts that constitute the crime. Some definitions are more inclusive; some, less so. The definition matters because it affects how identity theft is measured and how it can be combated.

"Identity" refers to the distinguishing character or personality of an individual. A person's true or inner identity—his or her thoughts, feelings, and preferences—is not directly observable. The outer identity is that by which others recognize the person. Imagine a list of all of a person's characteristics: birth date, eye color, address, parents' names, favorite color, bank account number, frequency of shopping at the local grocery store, etc. The list includes unchanging features (birth date, parents' names), behavioral patterns (frequency of shopping at the local grocery store), and identifiers assigned by others to recognize the individual (bank account number, Social Security number, driver's license number). Each item in the list is a piece of *personal identifying information* (PII), and the complete list is a representation of the person's identity. Others recognize the person by matching him or her against the parts of the list of which they have knowledge.[1] Friends, relatives, and co-workers tend to rely on physical features—the way the person

looks and the sound of his or her voice, for example—to identify the person. Parties with whom the person transacts rely on identifiers that work well remotely, such as name, address, phone number, and Social Security number. The subsets of PII that are used in transacting can be thought of as *transactional identities*.

Identity theft involves the theft of elements of a person's identifying characteristics (items in the list such as name, address, credit card number). The United States recognized identity theft as a crime in 1998, with passage of the Identity Theft and Assumption Deterrence Act (ITADA). Under the ITADA, "identity theft" is defined as the knowing transfer, possession, or usage of any name or number that identifies another person, with the intent of committing or aiding or abetting a crime. This definition is broad enough to encompass the theft of unique physical representations of a person, such as fingerprints or voice prints.[2, 3]

The ITADA definition encompasses the three types of identity theft that exist today. At one end of the spectrum, it includes a person's stealing multiple pieces of information about someone and assuming the other's transactional identity, opening ID cards and numerous accounts in the person's name and representing oneself as the other person. This is often referred to as "new account" theft. At the other end of the spectrum, identity theft includes the more traditional existing-account fraud, where information is stolen about some existing financial account and used to make transactions or access the account's funds.[4] This is known as "existing account" theft. A third type of identity theft is "synthetic" identity theft, which occurs when an identity thief combines stolen information with fictional information to create a new, fake identity.

There is debate about whether the ITADA definition is too broad. Financial institutions and other businesses and trade organizations argue that the definition should apply to the less frequently observed new-account fraud.[5] Lumping this type of fraud together with existing-account fraud is claimed to muddy discussions of possible solutions and efforts made to combat identity theft, which depend on the form the crime takes. It also makes identity theft appear to be more prevalent than if the more narrow definition, limited to existing-account fraud, were used, raising more alarm among the public than some observers find necessary. The latter argument, along with a desire by financial

institutions to minimize the perceived prevalence and seriousness of the crime, is likely driving the objections to the ITADA's definition of "identity theft."

Despite the objections, the more inclusive definition is appropriate because every bit of personal information that an identity thief obtains counts. Technology now allows people to share information and form networks, both personal and professional. This can enhance productivity and personal satisfaction, but there is a darker side to it as well: Identity thieves are leveraging any information they steal by using publicly available sources of information to fill in the blanks. For example, social networking sites, such as MySpace and Facebook, and online resumes provide information for those intent on identity theft. Newspaper websites commonly publish birth announcements, which include the newborn's birth date, city of residence, and the names of parents, grandparents, and siblings. This type of information readily allows a potential identity thief to identify the mother's maiden name of the newborn's siblings and parents. Obituaries and marriage announcements are also a source of information. One study found that a mother's maiden name can be inferred through automated searches of public records with alarming certainty.[6] Similar research regarding Social Security numbers (SSNs) is under way at Carnegie Mellon University.[7] From information publicly available from the U.S. Social Security Administration (SSA), an SSN can be matched to the issuing state and date, estimated age range of the recipient, and activity status. The goal of the research, as well as the SSA's provision of information for validating SSNs, is to improve identification of fraudulent SSNs. However, it also makes it easier for an identity thief to infer other personal information, such as place of birth.[8] Add in access by an identity thief to a LexisNexis account or to the database of a credit reporting agency or data broker, and compiling extensive information on a person is simple.[9]

Some retail establishments collect customer phone numbers or zip codes so they can more effectively use direct mail advertising and match customer traffic data to demographic data to better stock their stores. An identity thief who obtains electronic records containing a customer's name and phone number or zip code from a retail establishment's computers, even if the credit or debit card number were not stored, can use the reverse look-up feature of electronic telephone

books to match the phone number or zip code with the customer's address. Of course, the direct look-up feature can also be used to identify an address and phone number for people whose names appear in newspaper announcements of births, marriages, and deaths.

In short, it is easy to compile databases with increasingly complete records of individuals' information. All identity thieves need do is combine a little stolen PII with a lot of information publicly available to use themselves or sell to other identity thieves. Consequently, the common perception about identity theft is wrong. The theft of a few pieces of nonsensitive data, such as names, email addresses, and phone numbers, is not innocuous.[10] Even data intrusions in which little information is obtained can put victims at greater risk of having financial frauds committed in their names and with their accounts in the future. Thus, the more inclusive definition of "identity theft" is more appropriate: Identity theft is a crime against the owner of PII, and that person has no reason to distinguish thefts of a few pieces of PII that allow fraud on existing accounts from incidents of new-account fraud.

Individuals are not the only ones at risk. Nonconsumer entities (governments, businesses, educational institutions, and other entities) can be victimized also. Even computer security companies are at risk of others masquerading as them.[11] In addition, identity theft requires that such entities distinguish customers using false identities from legitimate customers, which raises the cost of transacting and hinders their ability to prevent fraud.

II. THE SCOPE OF THE PROBLEM

Identity theft has been around for at least as long as the paper check. In the last ten years, however, incidents of identity theft and the cost to the economy have grown dramatically. Only recently have data been collected on the scope of the problem, which is difficult to measure. Low-end estimates indicate costs to the U.S. economy alone of billions of dollars each year.

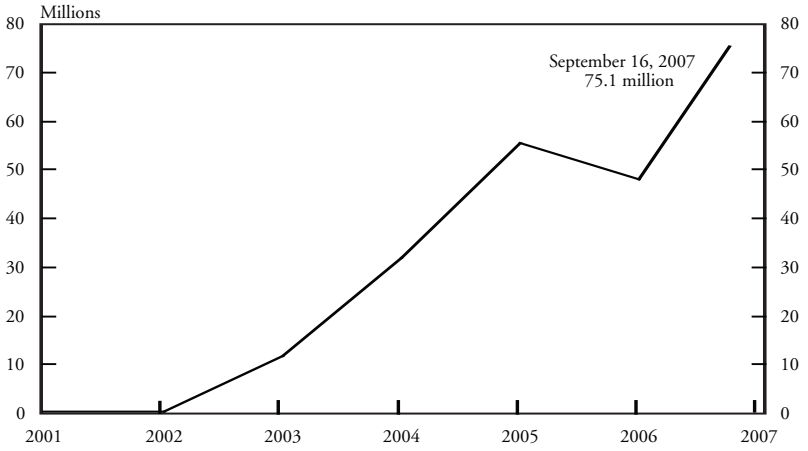
Quantifying identity theft

Efforts to track the growth in identity theft and in activities involving the theft of PII began only in the 21st century. The measures available are not completely reliable or easily compared to each other as they rely on sources such as surveys of consumers based on their own knowledge of whether they are victims, and reported incidents of data breaches or malicious computer activity by businesses and other entities. In addition, none of these measures captures synthetic identity theft, which often is not caught by a victim because the thief uses a mix of authentic and false information. By one estimate, more than 80 percent of all new-account identity theft has occurred using synthetic identities.[12] All of these measures therefore understate the problem, possibly dramatically.

Most of what is known about the prevalence of identity theft comes from annual surveys of consumers in recent years. One of the most recent surveys, conducted by Javelin Strategy & Research, found that in 2006 8.4 million U.S. consumers discovered themselves to be victims of identity theft. Through misuse of the stolen PII, identity thieves obtained $5,720 from the average victim. That implies total fraud of about $49.3 billion.[13, 14] Add to that the $4.9 billion that consumer victims incurred in out-of-pocket expenses to resolve the crime, and the market value of the hours spent on resolution activities, which totals $6.7 billion, and identity theft cost the U.S. economy about $61 billion in 2006.[15] The true economic cost is much larger because this calculation excludes the cost of incidents not known to victims at the time of the survey, the cost to consumers and businesses of security precautions to prevent future incidents of identity theft, insurance and litigation costs, and resolution costs incurred by businesses, for example. Some of the costs borne by businesses might be passed on to consumers in higher prices, interest rates, and fees.

Information on the number of data breaches from hacking incidents, loss or theft of storage devices, or other means, are available from *Attrition.org*, an information security-related website. *Attrition.org* has identified an explosion in the number of data breaches: 771 data

Chart 1
NUMBER OF RECORDS COMPROMISED



Source: www.attrition.org

breaches involving more than 221 million records through September 16, 2007. The percentage of breaches in which Social Security numbers were stolen has risen dramatically as well (Charts 1 and 2).

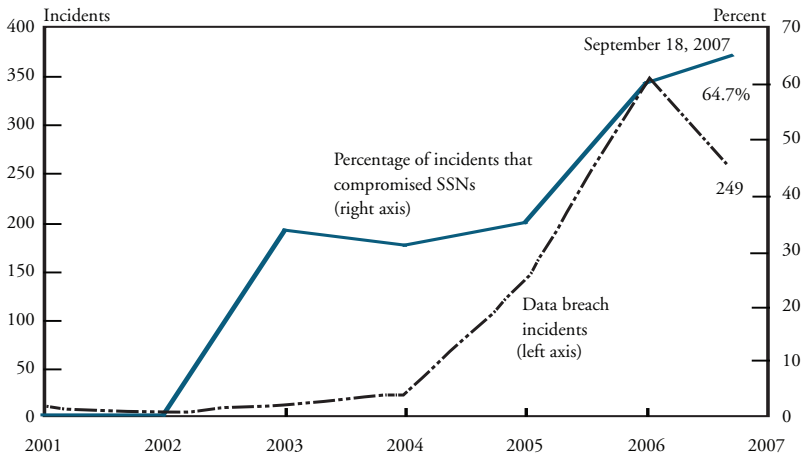
Attrition.org's data only include security breaches that are disclosed publicly, as is true for any measure of data breaches. Thus, the number of breaches and number of records compromised understate the true extent of the problem. The number of records compromised is understated to a greater extent because in many cases the number of records lost or stolen are unknown or not disclosed.

Survey data also provide some sense of the extent to which data breaches are occurring. Ponemon Institute polled 700 U.S. executives, managers, and IT security officers in midsized to large businesses across many industries in early 2007 and found rampant data breaches.[16] Eighty-five percent of respondents had experienced a data breach involving the loss or theft of PII in the previous two years, although less than 43 percent had a response plan in place to deal with data breaches, and 46 percent did not use encryption technology or conduct data security training after a breach.

The fact that records containing PII are lost or stolen does not equate to incidents of identity theft. As discussed in Section I, however, once a few pieces of information are stolen, other information can be

Chart 2

NUMBER OF REPORTED DATA BREACH INCIDENTS PER YEAR

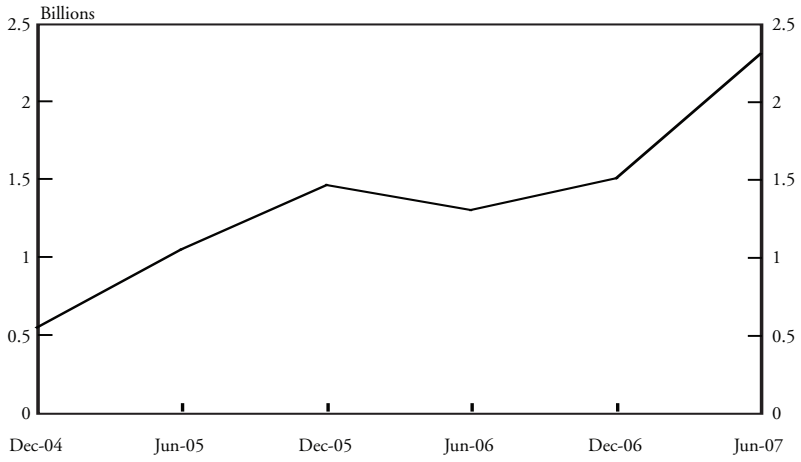


Source: www.attrition.org

obtained from public records or other data thefts and combined to obtain more complete identification records, increasing the odds that the owners of the information become victims of identity theft.

Phishing is an increasingly prevalent technique for potential thieves to acquire PII. Phishing refers to attempts by third parties to obtain confidential information by tricking a computer user into disclosing the information. Often an email is sent to the user that appears to be from a legitimate business with whom the computer user might do business. The email directs the user to take some action, such as responding to the email or going to a website identified in the email and providing personal information directly. Symantec, the Internet security firm, attempts to block phishing emails and has been tracking the number of emails blocked since 2004. The number of phishing attempts has risen dramatically since then (Chart 3). For the first six months of 2007, Symantec blocked more than 2.3 billion phishing emails, which averages to about 12.5 million emails per day.[17] The number of successful incidents is unknown. The sharp rise in phishing attempts in the first half of 2006 probably stems from the development

Chart 3
PHISHING EMAILS BLOCKED BY SYMANTEC



Source: Constructed from Symantec Internet Security Threat Reports from March 2005 through September 2007

of phishing kits that can be bought and easily downloaded from the Internet and installed automatically. These kits allow a novice to rapidly establish a phishing site.[18]

Thieves also frequent peer-to-peer (P2P) file-sharing networks through which participants share music and movies, searching for files on participants' computers containing tax returns, credit reports, Social Security numbers, and bank account information. P2P software, when loaded on a computer, allows others to access the computer to search for shared files. If the software is not installed properly or the computer is compromised by certain viruses, the machine's entire hard drive is accessible to anyone else on the networks. During a two-week period in late August and early September 2007, Tiversa, Inc., a company that monitors P2P networks, identified approximately 56,000 searches for the term "credit card," 75,000 searches for specific credit card statements, 50,000 searches for "tax returns," and 317,000 searches for "pin" and "user id."[19]

While the lack of accurate data hinders analysis of identity theft, it is clear that efforts to steal PII are ballooning, and the risk of becoming a victim is growing along with them.

Examples of recent identity theft incidents

Another way to understand the growth in data breaches and identity theft is through actual incidents. In 2007, data breaches at companies, educational institutions, and government agencies were announced almost daily. Two that involved identity theft—the TJX theft and the *Monster.com* breach—are highlighted here to illustrate the scope of the problem.

The TJX theft. On March 28, 2007, The TJX Companies Inc. (TJX), owner of T.J. Maxx, Marshall's, and other retailers, announced that it had been the victim of a data breach that began in July 2005 and continued into January 2007.[20] During that time, the hackers repeatedly accessed the company's main database, stealing files that contained information about transactions made with credit and debit cards and, for transactions involving returns, names, addresses, and drivers license numbers. It is believed that the hackers were able to decrypt whatever data were encrypted. This was the largest theft of customer data reported to date, with approximately 45.7 million credit and debit card numbers reported as stolen by TJX.[21]

The stolen PII has been used in fraudulent transactions worldwide.[22] In November 2005, customers of Fidelity Homestead, a Louisiana savings bank, started noticing charges on their credit and debit card statements for fraudulent purchases in Southern California. Those charges have been traced to the use of information from the TJX breach. In the fall of 2006, a crime gang in Florida rented cars and traveled to 50 of Florida's 67 counties, purchasing $8 million in $400 gift cards from Wal-Mart and Sam's Club stores with payment cards cloned using the stolen TJX information.[23] They then used the gift cards to purchase flat screen TVs, computers, and other electronics. The thieves had bought a batch of 10,000 of the stolen TJX payment card numbers via the Internet from a foreign source.

The Monster.com theft. Another large security breach occurred at *Monster.com*, the job-search website, and illustrates how a little information from what might appear to be an unlikely source can be used to do further harm.[24] On August 22, 2007, *Monster.com* announced that the PII of 1.6 million *Monster.com* users had been obtained from the company's resume database and used over the preceding six months in

phishing schemes. The thieves registered with *Monster.com* as employers looking for new employees in order to access the resume database. They collected users' names, email addresses, phone numbers, and the identification numbers of their online resumes. With this information, they sent various phishing emails to the individuals. One appeared to be a job offer, but required that the candidate be a Bank of America account holder and reveal the bank account number. Two other emails appeared to come from *Monster.com* and asked the recipient to download a new "Monster Job Seeker Tool." In one email, the link downloaded a keylogger program to the recipient's computer that recorded keystrokes typed into the user's computer, including online bank account numbers, log-in IDs, and passwords, and transmitted the information to the thieves. In the other email, the link downloaded ransomware, which encrypted files on the user's computer and held them for ransom. The emails appeared legitimate because they contained personal information about the users, such as the users' addresses and cell phone numbers, obtained, of course, through the initial breach of *Monster.com*'s database. The stolen information was traced to a computer outside the United States.

III. UNDERSTANDING IDENTITY THEFT'S RECENT GROWTH

The identity-theft crime wave has been made possible by a convergence of technological developments that have allowed the digitization and electronic storage of data, the conduct of routine financial transactions and recordkeeping by computer, and the creation of legal and illegal electronic markets in PII. As a result, identity theft has evolved from a crime that victimized isolated individuals to a lucrative, though illegal, business of organized crime rings. It has been fueled by legal sales of data that have created additional points of access for identity thieves.

Identity theft as digital burglary

The scope of the identity-theft problem can be seen by comparing the theft of PII to a traditional home burglary. A burglar breaks into a house to steal cash, jewelry, and other objects that can be sold for cash

or used by the burglar. During the break-in, the burglar also could steal physical pieces of personal and financial information—for example, a driver's license, Social Security card, a checkbook. With the identification documents in hand, the thief can commit fraud in the victim's name, whether on existing accounts or by opening new accounts. The burglar becomes an identity thief.

Before records were digitized and banking and shopping occurred remotely online, identity theft occurred on a fairly small scale. Home burglaries, for example, had to occur on site. Only one house could be burglarized at a time, with a thief having to go house to house physically removing items. Burglar alarms, barking dogs, vigilant neighbors, and noise from breaking into the house, as well as the need to be physically present to pawn or sell the stolen goods also limited acts of identity theft. Similarly, other common methods of stealing identifying information, such as stealing the carbon-copy imprints from credit card receipts, stealing PINs by looking over a cardholder's shoulder as the PIN is entered at the point of sale, and similar techniques, also had to be used in person, which limited the occurrence of identity theft by such means.

Identity theft still happens the old-fashioned ways, but today it mostly occurs digitally. The identity thief is most comparable to a burglar who only steals a spare key to the house so he can reenter whenever he wants and steal funds from the homeowner. By stealing individuals' PII, the identity thief essentially steals the keys to the individuals' financial accounts and credit ratings. With the information on a credit card, for example, the thief can clone the card and use the fake card to make a cash withdrawal from an ATM machine. Unlike the burglar, the identity thief can commit the crime many miles from the victim, and even from the privacy of the thief's home. The identity thief also can operate on a larger scale than the burglar, robbing many people at once, as when a hacker gains access to a computer database, downloads the PII of millions of individuals, and uses or sells it.

Technology-enabled identity theft

When identity theft is viewed as a form of digital burglary, it becomes clear that the crime now can occur at much lower cost and with a greatly reduced chance of arrest. It also can occur on a much larger scale, with millions of people and businesses victimized at once. These changes have come about as a result of technological developments that have altered the way payments are made and everyday life is conducted.

Although it is difficult to isolate technological developments that have enabled the growth of identity theft, three developments stand out as candidates. The first is the realization of Moore's law—the prediction that the number of transistors on a microprocessor would double about every two years.[25] Since 1965, when Gordon Moore made this prediction, computer processing speed has indeed increased exponentially and lowered computing costs accordingly. Increased computing power made possible comparable advances in memory capacity and most other features of computers. A small laptop computer can now perform functions and store data that in the 1970s required a mainframe computer.

The second development was improvements in connectivity and the communications it supports. The creation of TCP/IP and broadband (high-speed) Internet access were key. In the 1970s, researchers created TCP/IP, short for Transmission Control Protocol/Internet Protocol, a set of rules for connecting different networks into a network of networks—the Internet. IP is much like a postal system for the electronic exchange of information. It dictates the format of packets—chunks of data—that are sent between computers and the addresses for the computers. TCP allows distinct computers to connect to each other and exchange streams of data, guaranteeing accurate delivery of the packets. IP drops the packets in the postal system, while TCP makes the connection that allows the packets to be transferred between sender and recipient. Thanks to TCP/IP, any two people with Internet access can communicate and transfer information between them.

When TCP/IP was originally developed, people had to access the Internet over telephone lines; they would use a modem to dial into an Internet service provider's system to establish a modem-to-modem link, which was routed to the Internet. Data transfer was slow on these

systems. Since around 2000, broadband Internet access by cable or DSL has been replacing dial-up access. Broadband technology can transfer information at speeds far exceeding those for dial-up. Developments in fiber-optic communications helped make broadband Internet access much more cost effective over greater distances. With broadband, the connection is always there; no dialing up is necessary. If the computer is on, the connection is present.

As a result of these advances, powered-on computers around the world with Internet service are connected to each other, even when their users are not present. The link between computers also links people. It is beneficial in that it allows communication and information sharing among great numbers of people and across vast distances. It also allows more transactions to occur remotely as evidenced by the growth of e-commerce. These benefits, however, come at the cost of the user being exposed to computer intrusions and the interception of data in transit to others. Without effective security in place on a computer, anyone else with access to the Internet can directly access data on the computer.

The third development involves how people make transactions. Advances in telecommunications and computing accelerated the shift from cash transactions, which can be made anonymously, to transactions that require the transfer of PII to direct and authorize the transaction. The latter can be called *information-dependent transactions* and include transactions made with checks, credit cards, debit cards, and ACH. For example, in a credit-card transaction, the card provides information that allows it to be authenticated, both for the validity of the card number and the sufficiency of the amount of credit available through the card. Once authenticated, the card essentially issues a set of instructions directing the issuance of credit to the cardholder and transfer of borrowed funds to the seller. The card then directs the card issuer to bill the cardholder for the transaction according to the terms associated with the credit line to which the card gives access.

These developments together have dramatically changed the extent and uses to which people put computers. Consumers can now do their taxes, manage their finances, and shop by computer—and store information associated with each of those activities on their computers. Businesses can digitize their paper records and conduct transactions

with their customers by computer. More sensitive information can be stored on computers and sent between computers than ever before. And each computer is a potential source of PII for identity thieves.

The emergence of electronic markets in PII

Independently, the developments discussed above would not have fueled the growth of identity theft. Together, however, they have allowed the creation of legal and illegal electronic markets in PII.

Legal markets. Advances in computing power have allowed the digitization of paper records containing personal data. They also have allowed that data to be analyzed and packaged in innumerable ways. Data brokers purchase PII from credit reporting agencies and other entities, combine it with information acquired from public records, organize the information, and resell it to companies or government agencies seeking to conduct background checks or otherwise verify identities. Widespread, fast, and easy access to the Internet has allowed the data brokerage industry to thrive.[26]

Finding organizations willing to sell their customers' data is easy. For many entities, data are produced as a byproduct of their main line of business, with almost no additional costs of production, and they face fairly limited restrictions on their ability to resell the data. As a result, the resale to third parties can be an additional source of profit for them.

It should be no surprise then that state department of motor vehicles offices commonly sold driver's license records, sometimes including photographs, to data brokers, charities, political campaigns, and direct marketers. The Drivers Privacy Protection Act of 1994 was supposed to bring an end to such sales, but did not fully do so until the U.S. Supreme Court upheld the ban six years later.[27]

Financial institutions and other businesses also have been found selling customers' information.[28] The Gramm-Leach-Bliley Financial Services Modernization Act of 1999 somewhat restricted financial institutions' ability to use and share customers' financial information. The Act required these institutions to provide customers with a privacy notice indicating their intent to share information with third parties and offering customers the option of opting out of such data sharing.

Regulations adopted in late 2007 under the FACT Act (The Fair and Accurate Credit Transactions Act of 2003) also allow customers to opt out of a financial institution's use of information received from an affiliated company to market its products and services to customers.[29] Nonfinancial businesses, however, are not subject to these laws.

Illegal markets. The same technological developments that have fueled markets in the legal sale of PII also have spurred activity in illegal markets in PII. The casual hacker who once broke into computer systems for the challenge now can profit from his crime by selling the information, even if he never uses the stolen information himself to make fraudulent transactions. The online markets also provide a new source of profit for organized crime operations, allowing them to steal and sell personal information at low cost and on a large scale. The operation of legal markets in PII makes the identity thief's job even easier: It results in individuals' PII being more widely disseminated than it otherwise would be, which gives identity thieves more locations from which to access the information.

As with most underground markets, not much is known about how the markets in PII operate beyond what can be observed by those who gain access. Based on postings of PII offered for sale in September 2007, bank account data on an individual was selling for up to $400 per person, credit card details for up to $5 each, passwords for up to $350 each, and email addresses for between $2 to $4 per megabyte. "Complete identities" were available for $10 to $100 each.[30]

Pricing in these underground markets presumably reflects the expected benefit to the purchaser, the availability of the PII, and the expected cost of getting caught using the information. For example, financial account information, including passwords, allows immediate access to the funds in the account, partly explaining its higher price. In the case of brokerage accounts, the balance available to the thief can be quite large. In contrast, credit card information appears to be a volume business. Card information is easily obtained and often sold in bundles (such as the bundles of 10,000 card numbers from the TJX intrusion for sale). The sales price per number of cards is fairly low because the amount of available credit on the card accounts is unknown, the card issuer's fraud-prevention practices might detect fraudulent use at any time and deny further use of the card, and the cardholder might detect and report fraudulent use when the charges appear on the next card statement.

Information from credit cards for which further use has been denied is also being sold online. This is hard to explain unless the information bought is being used with other information to compile complete profiles on individuals. The sale of "full identities" is evidence of the success identity thieves are having at compiling fairly complete profiles.[31]

The benefit of hindsight

Identity theft is profitable precisely because today's economy is information dependent. Information flows where cash once changed hands at the point of sale. False information is the equivalent of counterfeit currency or stolen and forged checks. It is no wonder that identity theft is a problem of the modern payment system.

While the technological developments described above were occurring, they were not matched by comparable improvements in what can serve as transactional identities and how such identities are authenticated. Instead, practices that worked in a world of paper transactions were carried into the world of digital transactions, with dangerous consequences.

In the paper world, transactional identities were tied primarily to a single number—the Social Security number—and to a lesser extent to the driver's license number. People gave these numbers to businesses, governments, and other entities for use as record locators or as passwords, making the numbers means of identification and means of authentication. As a result, most other externally provided identifiers (credit card numbers, employee ID numbers) were tied to these two fundamental identifiers. The numbers would be recorded in the entity's paper records and stored. The records could be accessed, and stolen, but only by someone physically present where the records were stored, whether that person worked there or managed to gain access to them. Since the large-scale disappearance of paper records would likely be noticed, large-scale thefts of information were uncommon.

The digitization of paper records made larger thefts easier, but as long as computers were not connected, any theft had to occur on site, directly from the stand-alone computer storing the data. As computers became networked, both within an organization and to the world at large through the Internet, the possibility of the data stored on them being accessed by others soared. Without effective security measures in

place, anyone with the right skills could access the data. As the TJX data breach shows, the theft can occur remotely and involve enormous numbers of individuals' records.

The critical developments in computing, telecommunications, and payments technologies were not foreseen. Had they been, new methods of identification and authentication perhaps could have been developed early on and prevented digitized records from ever containing Social Security numbers and driver's license numbers, if appropriate. Property rights over one's own information could have been enhanced. Laws could have been passed regulating data security and clarifying privacy rights and liability for security lapses. The heightened conflict between individuals' desire for privacy and the government's need to accumulate PII for use in background checks and verifying identities as part of its national security efforts could have been considered directly, and perhaps more internally consistent policies could have been enacted.

IV. MARKET FAILURES AND IDENTITY THEFT'S RISK TO THE PAYMENT SYSTEM

In the absence of a technological development that makes identity theft undesirable by making it immediately traceable, just as caller ID virtually eliminated crank phone calls, some identity theft will likely always be present.[32] As with most other crimes, the costs of preventing identity theft will need to be balanced against the benefits of doing so to limit identity theft to an economically efficient degree.[33] If markets could achieve this efficient amount of identity theft, the government would not have to intervene, but this is not the case. Because asymmetric information and externalities are associated with the transfer and use of PII in making payments, the full cost of an act of identity theft will not be borne by those best positioned to prevent the theft, giving them too little incentive to protect against the crime. In addition, payment system integrity and efficiency are public goods—goods that markets tend to underproduce even in the absence of identity theft. Identity theft further threatens their provision, creating a role for government involvement.

Market failures associated with identity theft

For the competitive market to function efficiently, products have to be distinguished by their characteristics, including the risk associated with purchasing them, and their prices must reflect the cost of those characteristics.[34] This requires that all product features are known and their value to society captured in the purchase price. In markets with asymmetric information, sellers know more about their products, including the risks associated with purchasing them, than do buyers. When externalities are present, some benefits or costs of a transaction are borne by entities who are not parties to the transaction. As a result, products are not always priced efficiently.

Asymmetric information. Suppose a seller knows more about the quality of a good it is selling than its customers do. Assuming that sellers want customers to know of their goods' positive qualities, it is also reasonable to assume that sellers know the negative features of their goods but might not voluntarily inform customers of them. Under such conditions, a customer would pay a higher price for a good than if there had been full information about the good's features.

Asymmetric information comes into play regarding identity theft and the payment system because noncash transactions between a seller and customer involve the transfer of some of the customer's PII to effect payment. In essence, a transaction involves the purchase of both the product bought and the seller's protection of the customer's PII. The seller's safeguarding and use of customer data are material to the customer's evaluation of the cost of transacting with the seller. If the seller is lax in safeguarding its customers' information, then its customers are exposed to the risk of identity theft. The price a customer will pay for the seller's product should be reduced by the customer's expected cost from misuse of PII.

With asymmetric information, however, the seller knows more about how it uses and protects data than its customers do. Some sellers of otherwise identical products will spend more to protect consumer data better and will want to pass the extra cost onto their customers. Others will spend less on security and sell the same product at a lower price. If customers have full information about sellers' data security practices, customers valuing security more could buy the product at a

higher price from a seller offering better security; those who care less could purchase the product from a seller offering little security. Asymmetric information prevents customers from differentiating between sellers based on security practices. This forces customers instead to make purchase decisions based on their expected degree of data security across sellers, discounting purchases from all sellers by the same expected cost from misuse of PII. Consequently, different sellers' otherwise identical competing products will sell for the same price, regardless of how much security is conveyed with them. Sellers providing better security will earn a loss after data security costs are taken into account, while those providing lax security will earn a profit. Strong-security sellers thus have an incentive to provide less security. The industry as a whole is less secure as a result, and consumers desiring better security are unable to obtain it, even at a higher price. Such markets suffer from a "lemons problem," or *adverse selection*.[35] The result is that all sellers provide too little data security, resulting in too many data breaches and too much identity theft compared to what is economically efficient.

Externalities. Even without asymmetric information, markets can still fail to allocate resources efficiently when *externalities* are present. Externalities exist when the consumption or production of one person or entity affects another's, meaning that it confers benefits or costs on some other entity. Because some of the benefits or costs of an entity's actions are incurred by others, the entity does not consider them in its decision-making. The result is that the entity engages too heavily in activities that impose costs on others, and too little in activities that impose benefits on others.

Externalities are present in any market in which transactions involve a risk of data breaches and identity theft, even if sellers and buyers are equally well informed of a seller's data security practices. In the perfect (and nonexistent) world of full information about the risk of identity theft, sellers and buyers in principle can negotiate product prices or contract terms to compensate buyers for accepting the risk. Buyers might accept some risk in exchange for purchasing a product more cheaply, the exact price dependent on their perception of the cost to them of being a victim of identity theft. Buyers, however, have no reason to consider the cost that their agreed-to degree of risk will

impose on other entities, such as the cost to merchants and financial institutions from the fraudulent purchases made with the buyers' stolen PII, or the cost to taxpayers of having law enforcement entities catch and prosecute identity thieves. Because buyers do not incur these costs directly, they do not consider them when negotiating the risk-price trade-off associated with their product purchases. They accept too much risk from society's perspective.

Networks are prominent in the operation of the payment system, and they inherently involve externalities. Banks, payment processors, merchants, card associations, security firms, and Internet service providers all participate in one or more networks that process noncash payments. A data breach at any one can result in losses at the others, but individual participants will underinvest in data security because each pays the full cost of its investment but only receives part of the benefit from it; the rest of the benefit accrues to other network members and their customers.

A network's security is only as effective as the security of the weakest link—the participant most likely to experience a data breach.[36] Networks can adopt policies that impose minimum security practices or contractually assign liability for data breaches to improve within-network investment in security, but a network's security will still be too lax if the network's own breaches can impose losses on entities outside the network, including other networks, and the network does not bear the cost of those losses.

The TJX data breach, discussed above, illustrates the externalities associated with identity theft, even in a world with full and symmetric information. The breach exposed banks worldwide to costs from compromised cards that had to be reissued. A few months after the breach was announced, a coalition of more than 300 banks in New England, where TJX had a large share of its stores, filed a class action lawsuit to recover the cost of reissuing cards and of fraud. The total cost to the banking sector of reissuing cards could come to more than $1 billion. Fraud costs would be on top of that.[37]

Risks to the payment system

With externalities and asymmetric information associated with the transfer and storage of PII in noncash transactions, markets will not contain identity theft to an efficient degree. This threatens the integrity and efficiency of the payment system as well.

Integrity. Payment system integrity exists when system participants have confidence that they can make payments safely and reliably to execute transactions, when they trust that the payment system will operate as they expect it to. It is analogous to the confidence the public must have in the safety and soundness of the banking system for bank runs to not create systemic failure.

The integrity of the payment system is of critical importance because at the heart of a payment system is an economy's use of common means of payment, which facilitates trading among the economy's participants. People are willing to use a particular means of payment because they trust that others will accept it, and people accept it as payment because they trust that it has the value it is represented to have.

Coins and paper currency once were the common means of payment; they have been supplanted by the use of *credible promises to pay* (CPPs)—checks, credit cards, and debit cards. Use of these means of payment all result in the issuance of a promise to pay for a purchase in a particular way and within a particular time period. An extra degree of trust is involved with the use of CPPs because users must trust that the promises that CPPs embody will be fulfilled—in other words, that the CPPs were not issued fraudulently.

Identity theft challenges the trust that supports the payment system in two ways. First, it creates fears of victimization. Second, it reduces the effectiveness of established methods for authenticating transactions and thus the safety and reliability of the payment system. If trust is lost, people will be less willing to accept CPPs as payment, leading fewer people to use them. Markets can cease operation or revert to relying on methods of payment that are not dependent on the transmission of as much PII. The overall level of economic activity may be reduced, affecting many people besides those victimized by identity theft.

Efficiency. An efficient payment system minimizes the resources used in making and processing transactions. If a lack of payment system integrity causes people to avoid certain means of payment because of their high fraud rates or high security costs, that alone reduces a payment system's efficiency. For example, people could shift from using credit and debit cards to using more paper checks or cash. There might be less electronic bill payment than would otherwise have occurred, or less use of ATMs and greater use of bank branch services. Identity theft might result in people not shopping online as much as they might do otherwise. Evidence already exists of these effects. A *Wall Street Journal Online*/Harris Interactive Personal Finance Poll taken in May 2006 found that 30 percent of respondents limited the purchases they make online, while 24 percent limit their online banking transactions.[38] Such distortions in people's methods of making payment and shopping and banking practices are an inefficiency in the operation of the payment system.

The risk identity theft poses to the efficiency of the payment system when information-dependent transactions predominate resembles the risk from counterfeiting in an economy in which currency is the primary means of payment. In U.S. history, the most similar period was the Free Banking Era, from 1837 to 1863, during which time entry into banking was relatively free and banks issued their own currency. Counterfeiting was not rampant; in fact, wildcat banks—those that issued currency and shut down operations before redeeming it—were relatively rare in the Free Banking Era.[39] Transaction costs, however, were relatively high. Lists of illegitimate currency were published in bank-note reporters, which people would look to in deciding whether to accept unrecognized currency. Some would argue that even these transaction costs were relatively low. Still, every economy has moved toward a single, uniform currency when able, eliminating the bulk of such transaction costs. The European Union's introduction of the euro is a modern-day example.

Another market failure. Markets cannot ensure the optimal provision of payment system integrity or efficiency due to two features that make them *public goods*. First, no one can be prevented from consum-

ing them once they are supplied. Second, one person's consumption does not limit any other's. Public art and national defense share these features and are classic public goods.

The optimal supply of a public good will depend on the benefit of the good to all consumers jointly. The total benefit, however, cannot be realized by any single private market participant because free-riding is possible: People can consume the good without paying for it. This results in markets supplying too little of public goods, including payment system integrity and efficiency.

Market solutions and the role for government

The preceding discussion of market failures is not meant to suggest that the private sector does not spend considerable resources to prevent identity theft. Rather, it indicates that the private sector will not be able to do enough, due to market failures, to adequately protect the integrity and efficiency of the payment system.

One step the private sector has taken toward containing identity theft is the adoption of industry standards for data security.[40] These standards specify what data are stored, encryption standards, and penalties for noncompliance. To be effective, however, there must be some monitoring of compliance, and the penalties must be sufficiently high given the odds of being caught.[41] For example, the Federal Trade Commission's settlement with BJ's Wholesale Club, Inc. is an example of a fairly high penalty, although not one imposed by the private sector. In response to the FTC's allegations that BJ's failed to encrypt or properly secure customer data and wireless networks, BJ's was required to implement a broad information security program and have the program audited every other year for 20 years.[42]

Payment system participants also can hold each other accountable for damage from lax security procedures through their contractual arrangements. However, many system participants have access to customer payment data between the point of sale and final settlement, and few of them can anticipate their ultimate ties to each other and enter into contractual agreements that allocate the risk of harm from others' data security failures. The law in most states bars claims for recovery

brought on theories other than breach of contract.[43] As a result, payment system participants have difficulty recovering damages from identity theft through litigation.[44]

Losses from identity theft also can be difficult to recover because proving the damage can be difficult. In *Smith v. Chase Manhattan Bank,* 741 N.Y.S. 2d 100 (App. Div. 2002), a class of bank customers sued the bank for selling PII to third parties, including telemarketing firms. The case was dismissed because the court found that none of the customers had alleged receiving unwanted telephone solicitations or junk mail as a result of the data sales. In *Kahle v. Litton Loan Servicing LP*, S.D. Ohio, No. 1:05CV756 (May 16, 2007), the court found that customers cannot file suit for the threat of future harm from the theft of hard drives stolen from the loan servicing facility where there was no evidence that the information had been used fraudulently.

Although recovering on claims can be difficult, defending against them is nevertheless expensive. Consequently, news of the TJX data breach and other prominent breaches prompted calls for additional security measures. Merchants have called for new policies that allow them to discard payment card transaction data sooner. Other nonconsumer entities are also rethinking their data collection policies. PII cannot be stolen if it was never collected or retained.

Another fairly recent step taken by the private sector is the development of insurance products to cover losses from identity theft. Coverage for consumers is available from several sources, at a cost of approximately $120 per year, and appears to provide minimal coverage against lost wages, legal fees for defending against lawsuits brought by creditors or collection agencies, and select out-of-pocket expenses. Notably absent is coverage for losses from fraudulent charges.[45] Businesses are also becoming more interested in insuring against costs incurred in responding to data breaches.[46] Neither type of insurance will protect against identity theft's risk to the payment system, which is an aggregate and a systemic risk, because the private sector cannot insure against such risks. For example, identity theft insurance is comparable to airline flight insurance that reimburses policyholders' damages in the event of plane crashes, lost or stolen luggage, etc. Such insurance will not prevent policyholders from losing confidence in the

safety of air travel and choosing to travel less or by less efficient means if there are frequent plane crashes. This is the systemic aspect of the problem. Similarly, identity theft insurance reimburses certain damages incurred by policyholders but does not address the risk to the payment system from a loss of confidence. Something more like deposit insurance is needed to deal with systemic risk to the payment system.

Despite the effort the private sector puts into data security and the prevention of identity theft, the integrity and efficiency of the payment system are public goods that the government has an incentive to ensure are adequately provided. Disclosure requirements to reduce the asymmetric information problem, the clear and comprehensive assignment of liability to address externalities, and other policy interventions that would work much as a lender of last resort or deposit insurance work to prevent financial instability—these are just a few examples of the role that remains for government in addressing identity theft's impact on the payment system. Because government intervention brings with it its own share of inefficiencies, policy options must be weighed carefully before implementation.

V. CONCLUSION

Identity theft costs the U.S. economy alone billions of dollars each year. Advances continue in computer processing speed, communications capabilities across markets, and consumer and business payment methods. Together, these advances have changed dramatically the functions for which people use computers and have allowed legal and illegal markets in PII to arise, fueling identity theft. Imperfections in markets for goods and services contribute to the problem by limiting markets' ability to provide sufficient protection against the crime. This creates a role for government in overcoming these market failures with an eye to protecting the integrity and efficiency of the payment system.

Current government efforts to control identity theft almost exclusively take the form of consumer protections, law enforcement initiatives, and regulatory oversight of banks and their affiliates. These efforts assist individual victims and aim to prevent the use of identity theft in money-laundering schemes, schemes often used to fund the drug trade and terrorism, but do not adequately address the market

failures associated with asymmetric information, externalities, and the provision of public goods. The challenge is for government to find an appropriate way to protect the integrity and efficiency of the payment system from the risks of identity theft.

ENDNOTES

[1]Charles M. Kahn and William Roberds, "Credit and Identity Theft," Federal Reserve Bank of Atlanta Working Paper 2005-19, August 2005.

[2]The Identity Theft and Assumption Deterrence Act defined "identity theft" as occurring when someone "knowingly transfers, possesses, or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable state or local law." 18 U.S.C. §1028(a)(7) "Means of identification" include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual, including any—(A) name, Social Security number, date of birth, official state or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number; (B) unique biometric data, such as fingerprint, voice print, retina or iris image, or other unique physical representation; (C) unique electronic identification number, address, or routing codes; or (D) telecommunication identifying information or access device (as defined in section 1029(e))." "Access device" in 18 U.S.C. §1029(e)(1) is defined as used in 18 U.S.C. §1028(a)(7)to be "any card, plate, code, account numbers; electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)."

[3]"Identity theft" is also defined in the Fair Credit Reporting Act (FCRA), 15 U.S.C. §1681a(q)(3), and in the Federal Trade Commission's refinement of that definition in 16 CFR 603.2. The purpose of the FCRA is to "require that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance, and other information in a manner which is fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information in accordance with the requirements of this title." The FCRA achieves its goals, in part, by allowing consumers who have been or believe that they are about to become victims of fraud or a related crime, including identity theft, to direct a consumer reporting agency to put a fraud alert in the consumer's file and to obtain a free copy of the report (15. U.S.C. §1681c-1). It also directs consumer reporting agencies to block the reporting of any information in the file of a consumer that the consumer identifies as information that resulted from an alleged identity theft (15 U.S.C. §1681c-2). Consistent with these provisions to assist consumers who are victims of identity theft, the FCRA defines "identity theft" more narrowly than the ITADA, taking it to be a fraud committed or attempted using the identifying information of another person without authority (16 CFR §603.2). Because the FCRA's goal is not to recognize identity theft as a crime, the Act need not define "identity theft" from the perspective of the thief's actions, as the ITADA does, including the knowing transfer and possession of PII with the intent of aiding or abetting a crime.

[4]Medical identity theft works differently. With medical identity theft, the thief goes after the medical benefits of the victim, stealing information about insurance coverage and some identifying information and using the health insurance coverage in the victim's name. This article addresses only acts of identity theft that involve theft from financial accounts, including charge accounts. However, much of the article applies to medical identity theft as well.

[5]Julie Cheney, "Identity Theft: Do Definitions Still Matter?" Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper, August 2005.

[6]Virgil Griffith and Markus Jakobsson, "Messin' with Texas: Deriving Mother's Maiden Names Using Public Records," *CryptoBytes*, Winter 2007, RSA Laboratories, available at *www.rsa.com/rsalabs/node.asp?id=2149*.

[7]See *http://privacy.cs.cmu.edu/dataprivacy/projects/ssnwatch/index.html#overview*, the Carnegie Mellon Data Privacy Lab's website.

[8]An employee of a cell phone provider recently told the author that the company was moving away from the use of the last four digits of customers' Social Security numbers as the default password for customers' accounts because the numbers had been "totally compromised."

[9]In recent years, data breaches have been disclosed at data broker ChoicePoint and at LexisNexis. See for example Joshua Pantesco, "FTC imposes record fine on ChoicePoint in data-loss case," *Jurist*, January 26, 2006, *http://jurist.law.pitt.edu/paperchase/2006/01/ftc-imposes-record-fine-on-choicepoint.php*; Harry R. Weber, "ChoicePoint was victim of ID theft in '02," *The Seattle Times*, March 3, 2005, *http://seattletimes.nwsource.com/cgi-bin/PrintStory.pl?document id=2002195125&s lug=c …*; CBS News, "Hackers Hit Lexis Nexis Database," March 10, 2005, *http://www.cbsnews.com/stories/2005/03/10/tech/main679237.shtml*; Caleb Silver, "LexisNexis acknowledges more ID theft," CNN Money.com, June 2, 2005, *http://money.cnn.com/2005/04/12/technology/personaltech/lexis/*.

[10]Josh Funk, "Contact Data for Millions of Ameritrade Customers Stolen," *Kansas City Star*, September 14, 2007, *www.kansascity.com/business/vprint/story/276100.html*.

[11]For example, on February 9, 2007, VeriSign, a leading provider of critical infrastructure and Internet security services and the "trusted third party" that provides the "Verified by VeriSign" certification for websites, was the victim of a spoofing attack in which emails were sent to VeriSign customers that appeared to be from VeriSign and directed recipients to upload a file as part of VeriSign's new security procedures. The file, if uploaded, allowed the true sender remote access to the user's computer. See VeriSign's announcement of this at *www.verisign.com/support/alerts/ua-alerts/040713.html*.

[12]Stephen Coggeshall, "ID Theft Knows No Boundaries," *eCommerce Times*, April 13, 2007, *www.ecomercetimes.com/story/56864.html*. As an example of how synthetic identity theft can work, see "Victim of synthetic identity theft leaves no stone unturned," September 2007, available on the Identity Theft 911 website at *www.identitytheft911.org/articles/article.ext?sp=10223*.

[13]Javelin Strategy & Research, "Identity Fraud Is Dropping According to New Research," February 1, 2007, p. 2, *www.javelinstrategy.com/idf2007*. Privacy Rights Clearinghouse, "How Many Identity Theft Victims Are There? What IS the Impact on Victims?" October 18, 2007, *www.privacyrights.org/ar/idtheftsurveys.htm*, which reports results from the Javelin survey. Javelin's estimate of total fraud from identity theft of $49.3 billion is a three-year moving average of its sur-

vey results. Javelin made a methodological change in its survey for 2006 that reduced its original estimate by 40 percent. By taking a three-year moving average, Javelin smoothes its estimates across years, making the trend more plausible.

A similar survey by Gartner, Inc., found 15 million victims from August 2006 through August 2007, with the loss per victim of $3,257. Interestingly, the total amount of fraud also adds up to about $49 billion. Avivah Litan, "The Truth Behind Identity Theft Numbers," Gartner, Inc., February 28, 2007, p. 2.

The Javelin and Gartner surveys, like all others conducted, have limitations. For example, they only measure incidents of identity theft that have been discovered by consumers.

[14] The Federal Trade Commission conducted the first survey of identity theft in 2003 and conducted another survey in 2006. The 2006 survey results, which explore the incidence of identity theft in 2005, were released on November 27, 2007, as this article was going to press. Since 2003, private-sector research firms have conducted virtually the same survey. Javelin's survey was conducted most consistently since 2003 and provides results through 2006, so its results are discussed in the article. A brief review of the 2006 FTC survey results reveals that several significant methodological changes were made to the survey. These changes contribute to the FTC's estimate of $15.6 billion in fraud from identity theft in 2005 being so different from private-sector estimates of about $50 billion for that year and from its own estimate of $33 billion for 2002 (obtained from its 2003 survey). The FTC's 2006 report advises that based on changes in the methodology of its survey between 2003 and 2006, it cannot determine whether total fraud has actually dropped significantly since 2003. (Synovate, "Federal Trade Commission—2006 Identity Theft Survey Report," November 2007, p. 9.)

[15] Javelin surveyed 5,006 consumers, and 458 of them reported being a victim of identity theft in 2006. Extrapolated to the population as a whole, Javelin reports that 8.4 million U.S. consumers were victims of identity theft in 2006. One percent reported being victims of new account fraud and spent, on average, $792 out of pocket to resolve the crime. An average of $587 was spent on out-of-pocket expenses to deal with existing-account fraud. However, a victim who experienced both new and existing account fraud had their out-of-pocket costs counted by Javelin as spent wholly on resolving new account fraud and also wholly on resolving existing account fraud. To offset possible double counting, this article takes $587 to be the out-of-pocket cost by each of the 8.4 million victims, generating the $4.9 billion estimate of total out-of-pocket expenses for resolution.

In addition, Javelin reported that the average victim spent 25 hours resolving the crime. The median victim spent five hours. For the lowest-income consumers, those with incomes at or below $15,000, which is approximately the income of a full-time worker earning the federal minimum wage of $7.25 per hour, the average resolution time was 44 hours. In 2006, the average U.S. household earned $66,570, or $32 per hour in a 40-hour per week job (average income from U.S. Census Bureau, "Income, Poverty, and Health Insurance Coverage in the United States: 2006," August 2007, Table A-1). At that hourly wage, the 25 hours spent by the average victim on resolution had a market value of $800. This implies that total resolution time cost the economy $6.7 billion.

[16] Alexei Alexis, "Data Security Breaches Rampant Among Businesses, Survey Shows," *Banking Daily*, May 15, 2007.

[17]Dean Turner, Stephen Entwisle, and Eric Johnson, eds., "Symantec Internet Security Threat Report, Trends for January-June 07," September 2007, p. 95, *www.symantec.com/content/en/us/about/media/ISTRXII_Main.pdf.*

[18]Daniel Wolfe, "New Phishing Kits Ease Way for Amateurs," *American Banker*, vol. 172, No. 130, July 9, 2007.

[19]"Federal Grand Jury Indicts Man for Allegedly Using Consumer Information from P2P File Sharing Networks to Commit ID Theft and Fraud; Man Allegedly Used Tax Returns, Bank Statements, and Credit Reports to Establish Identities to Defraud Consumers, Banks, and Retailers—Thousands of Potential Criminals a Day Use P2P to Mine Consumer Information Needed to Commit ID Theft and Fraud," *PR Newswire*, September 6, 2007, and *www.tiversa.com.*

[20]The discussion of the TJX theft is based on: Donald G. Aplin, "TJX Says at Least 46.2 Million Credit Cards Affected in Computer Hack, FTC Investigating," *Banking Daily*, March 30, 2007; Larry Greenemeier, "Data Theft, Pushback, and the TJX Effect–Details of the largest customer data heist in U.S. history are beginning to emerge," *InformationWeek*, August 13, 2007; Joseph Pereira, "Breaking The Code: How Credit-Card Data Went Out Wireless Door—Biggest Known Theft Came From Retailer With Old, Weak Security," *The Wall Street Journal*, May 4, 2007; United States Securities and Exchange Commission, The TJX Companies, Inc. *Form 10-K. Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934* for the fiscal year ended January 27, 2007, published March 28, 2007; and Daniel Wolfe, "Security Watch," *American Banker* 172, no. 162 (2007), August 22, 2007.

[21]Banks that have filed suit against TJX to recover the costs they incurred from reissuing credit and debit cards and fraudulent purchases have alleged that 94 million payment card accounts were compromised as a result of the data breach. The accounts breached include about 65 million Visa cards and 29 million MasterCards. See "TJX Fights Class Certification of Banks: Plaintiffs Say Breach Larger Than Admitted," *Banking Daily*, October 25, 2007, and Daniel Wolfe, "94M Accounts in Breach?" *American Banker*, October 25, 2007.

[22]Robert Lemos, "Fraud linked to TJX data heist spreads," *SecurityFocus*, January 26, 2007, *www.securityfocus.com/print/news/11438*, citing reports of stolen credit cards used in Hong Kong, Sweden, and three U.S. states.

[23]Evan Schuman, "Stolen TJX Data Used in $8M Scheme before Breach Discovery,"*eWeek*, March 21, 2007, *www.eweek.com/print_article2/0,1217,a=203568,00.asp.*

[24]This discussion is based on Rochelle Garner, "Monster.com Users Get Fake Offers and Request," *The Washington Post*, August 23, 2007; Joseph Menn, "Thieves target Monster.com users," *The Los Angeles Times*, August 23, 2007; Joseph Menn, "Monster.com to notify 1.3 million theft victims," *The Los Angeles Times*, August 24, 2007; Daniel Wolfe, "Security Watch," *American Banker* 172, no. 162 (2007).

[25]Gordon E. Moore, "Cramming more components onto integrated circuits," *Electronics*, vol. 38, no. 3, April 19, 1965, *http://download.intel.com/research/silicon/moorespaper.pdf.*

[26]Nathan Brooks, "Data Brokers: Background and Industry Overview," Congressional Research Service, Library of Congress, May 5, 2005, *www.opencrs.com/rpts/RS22137_20050505.pdf.*

[27]Kris Hundley, "Florida has sold license photos," *St. Petersburg Times*, January 23, 1999; Linda Greenhouse, "Justices uphold ban on states' sales of drivers' license information," *The New York Times*, January 13, 2000.

[28]See Holden Lewis, "Banks are selling your private information," Bankrate.com, *www.bankrate.com/brm/news/bank/19991008.asp*, October 8, 1999; Russell Mokhiber, "Bank Privacy Sold Out," *Multinational Monitor*, June 1999, *http://multinationalmonitor.org/mm1999/99june/front2.html*; "First USA Pays $1.3 Million to Settle Deceptive Practices Case," April 22, 2003, Consumeraffairs.com.

[29]"Agencies Issue Final Rules on Affiliate Marketing," Joint Press Release of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision, October 25, 2007, *www.federalreserve.gov/newsevents/press/bcreg/20071025a.htm.*

[30]Dean Turner, Stephen Entwisle, and Eric Johnson, eds.,"Symantec Internet Security Threat Report: Trends for January-June 07," September 2007, p. 44, *www.symantec.com/content/en/us/about/media/ISTRXII_Main.pdf.*

[31]A telephone conversation on June 19, 2007, with Dan Clements of Card Cops, *www.cardcops.com*, was the source for some of the information on the operation of the electronic markets in PII.

[32]Caller ID eliminated crank phone calls but not unwelcome telemarketing calls because telemarketing is fundamentally different than harassment and identity theft. The telemarketer wants to sell something, which requires the caller identifying himself. The maker of a crank phone call, like the identity thief, has no desire to identify himself. Consequently, the development of caller ID was sufficient to eliminate crank phone calls, but the creation of a national Do Not Call List and government regulations penalizing telemarketing calls to people on the list were needed in addition to caller ID to reduce the number of telemarketing calls.

[33]Charles M. Kahn and William Roberds, "Credit and Identity Theft," Federal Reserve Bank of Atlanta Working Paper 2005-19, August 2005.

[34]This article refers only to products or goods, but the discussion applies equally to the provision of services.

[35]George Akerlof, "The Market for Lemons: Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, August 1970, 84 (3): 488-500.

The presence of a lemons problem with respect to data security can make it appear that customers do not value data security or are unwilling to pay for it when they actually do value it. See Adam Shostack and Paul Syverson, "What Price Privacy?" in *Economics of Information Security*, editors L. Jean Camp and Stephen Lewis, Springer, 2004.

[36]Hal Varian, "System Reliability and Free Riding," *Mimeo*, November 30, 2004.

[37]Massachusetts Bankers Association, "Massachusetts, Connecticut Bankers Associations and the Maine Association of Community Banks and Individual Banks File Class Action Lawsuit Against TJX Companies Inc.," press release, April 24, 2007.

[38]Jennifer Cummings, "Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft," *The Wall Street Journal Online/Harris Interactive Personal Finance Poll*, May 18, 2006.

[39]Arthur J. Rolnick and Warren E. Weber, "New Evidence on the Free Banking Era," *American Economic Review*, vol. 73, no. 5, December 1983, 1080-1091.

[40]See, for example, the PCI Data Security Standard at *www.pcisecuritystandards.org.*

[41]Banks suing TJX to recover damages incurred from the TJX data breach allege that TJX did not follow credit card industry data security standards and was aware of its computer network's vulnerabilities before the breach. "TJX failed most PCI data security standards, knew of risks before breach, banks assert," *Banking Daily*, October 31, 2007.

[42]Thomas Claburn, "BJ's Wholesale Club Settles FTC Data-Protection Complaint," *Information Week*, June 16, 2005.

[43]In most states, the Economic Loss Doctrine is applied to bar most tort claims for purely economic losses, and identity theft imposes economic losses.

[44]See Gary Clayton, "Privacy and Security Litigation and Enforcement: Growing Risks for Businesses?" International Risk Management Institute, May 2007, *www.irmi.com/Expert/Articles/2007/Clayton05.aspx*; *Sovereign Bank v. BJ's Wholesale Club, Inc.*, 427 F.Supp.2d 526 (M.D. Pa., 2006); and *Banknorth, N.A. v. BJ's Wholesale Club, Inc.*, 442 F.Supp.2d 206 (M.D. Pa., 2006).

[45]Covered out-of-pocket expenses are those for long-distance phone calls, postage, reapplication fees, notary fees, and credit reports. Expenses for fraudulent charges, withdrawals, loans, utility bills, or other accounts opened by an identity thief are not covered. The difference between a homeowner's insurance policy and identity theft insurance is that when the house of a homeowner's insurance policyholder is robbed or damaged by a storm, the policy reimburses the policyholder for the value of the stolen or damaged items

[46]Louise Esola, "Banks consider identity theft cover as criminals target data; Information security becomes big concern as losses mount," *Business Insurance*, February 26, 2007, vol. 41, no. 9, p. 20.

REFERENCES

Akerlof, George. 1970. "The Market for Lemons: Quality Uncertainty and the Market Mechanism," *Quarterly Journal of Economics*, vol. 84, no. 3, August, pp. 488-500.

Alexis, Alexei. 2007. "Data Security Breaches Rampant Among Businesses, Survey Shows," *Banking Daily*, May 15.

Aplin, Donald G. 2007. "TJX Says at Least 46.2 Million Credit Cards Affected in Computer Hack, FTC Investigating," *Banking Daily*, March 30.

Banking Daily. 2007. "TJX Failed Most PCI Data Security Standards, Knew of Risks before Breach, Banks Assert," October 31.

_____. 2007. "TJX Fights Class Certification of Banks: Plaintiffs Say Breach Larger Than Admitted," October 25.

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision. 2007. "Agencies Issue Final Rules on Affiliate Marketing," Joint Press Release, October 25, *www.federalreserve.gov/newsevents/press/bcreg/20071025a.htm.*

Brooks, Nathan. 2005. "Data Brokers: Background and Industry Overview," Congressional Research Service, Library of Congress, May 5, *www.opencrs.com /rpts/RS22137_20050505.pdf.*

CBS News. 2005. "Hackers Hit Lexis Nexis Database," March 10, *www.cbsnews.com/stories/2005/03/10/tech/main679237.shtml?source=search_story.*

Cheney, Julie. 2005. "Identity Theft: Do Definitions Still Matter?" Payment Cards Center, Discussion Paper, August.

Claburn, Thomas. 2005. "BJ's Wholesale Club Settles FTC Data-Protection Complaint," *Information Week*, June 16.

Clayton, Gary. 2007. "Privacy and Security Litigation and Enforcement: Growing Risks for Businesses?" International Risk Management Institute, Expert Commentary, May, *www.irmi.com/Expert/Articles/2007/Clayton05.aspx*

Clements, Dan. 2007. Telephone conversation, June 19.

Coggeshall, Stephen. 2007. "ID Theft Knows No Boundaries," eCommerce Times, April 3, *www.ecommercetimes.com/story/56864.html.*

Consumeraffairs.com. 2003. "First USA Pays $1.3 Million to Settle Deceptive Practices Case," April 22, *www.consumeraffairs.com/news03/first_usa.html.*

Cummings, Jennifer. 2006. "Substantial Numbers of U.S. Adults Taking Steps to Prevent Identity Theft," *The Wall Street Journal Online/Harris Interactive Personal Finance Poll*, May 18.

Esola, Louise. 2007. "Banks Consider Identity Theft Cover As Criminals Target Data; Information Security Becomes Big Concern as Losses Mount," *Business Insurance*, vol. 41, no. 9, February 26, p. 20.

Funk, Josh. 2007. "Contact Data for Millions of Ameritrade Customer Stolen," *Kansas City Star*, September 14.

Garner, Rochelle. 2007. "Monster.com Users Get Fake Offers and Request," *The Washington Post*, August 23.

Greenemeier, Larry. 2007. "Data Theft, Pushback, and the TJX Effect—Details of the largest customer data heist in U.S. history are beginning to emerge," *InformationWeek*, August 13.

Greenhouse, Linda. 2000. "Justices Uphold Ban on States' Sales of Drivers' License Information," *The New York Times*, January 13.

Griffith, Virgil, and Markus Jakobsson. 2007. "Messin' with Texas: Deriving Mother's Maiden Names Using Public Records," *Cryptobytes*, RSA Laboratories, vol. 8, no.1, Winter, pp. 18-28, *www.rsa.com/rsalabs/cryptobytes/-CryptoBytesWinter07.pdf*.

Hundley, Kris. 1999. "Florida Has Sold License Photos," *St. Petersburg Times*, January 23.

Identity Theft 911. 2007. "Due Vigilance," September, *www.identitytheft911.org/articles/article.ext?sp=10223*.

Javelin Strategy & Research. 2007. "Identity Fraud is Dropping According to New Research," February 1, *www.javelinstrategy.com/idf2007*.

Kahn, Charles M., and William Roberds, 2005. "Credit and Identity Theft," Federal Reserve Bank of Atlanta, Working Paper 2005-19, August.

Lemos, Robert. 2007. "Fraud Linked to TJX Data Heist Spreads," SecurityFocus, January 26, *www.securityfocus.com/print/news/11438*.

Lewis, Holden. 1999. "Banks Are Selling Your Private Information," Bankrate.com, October 8, *www.bankrate.com/brm/news/bank/19991008.asp*.

Litan, Avivah. 2007. "The Truth Behind Identity Theft Numbers," Gartner, Inc., Research ID no. G00146532, February 28.

Massachusetts Banker Association. 2007. "Massachusetts, Connecticut Bankers Associations and the Main Association of Community Banks and Individual Banks File Class Action Lawsuit against TJX Companies, Inc.," Press Release, April 24.

Menn, Joseph. 2007. "Monster.com to Notify 1.3 Million Theft Victims," *The Los Angeles Times*, August 23.

_____. 2007. "Thieves Target Monster.com Users," *The Los Angeles Times*, August 23.

Mokhiber, Russell. 1999. "Bank Privacy Sold Out," Multinational Monitor, vol. 20, no. 6, June. *http://multinationalmonitor.org/mm1999/99june/front2.html*.

Moore, Gordon E. 1965. "Cramming more components onto integrated circuits," *Electronics*, vol. 38, no. 3, April 19, *http://download.intel.com/research/silicon/moorespaper.pdf*.

Pantesco, Joshua. 2006. "FTC Imposes Record Fine on ChoicePoint in Data-loss case," *Jurist*, University of Pittsburgh Law School, January 26, *http://jurist.law.pitt.edu/paperchase/2006/01/ftc-imposes-record-fine-on choicepoint.php*.

Pereira, Joseph. 2007. "Breaking the Code: How Credit-Card Data Went Out Wireless Door—Biggest Known Theft Came From Retailer With Old, Weak Security," *The Wall Street Journal*, May 4.

Privacy Rights Clearinghouse. 2007. "How Many Identity Theft Victims Are There? What IS the Impact on Victims?" October 18, *www.privacyrights.org/ar/idtheftsurveys.htm*.

PR Newswire. 2007. "Federal Grand Jury Indicts Man for Allegedly Using Consumer Information from P2P file Sharing Networks to Commit ID Theft and Fraud; Man Allegedly Used Tax Returns, Bank Statements and Credit

Reports to Establish Identities to Defraud Consumers, Banks, and Retailers—Thousands of Potential Criminals a Day Use P2P to Mine Consumer Information Needed to Commit ID Theft and Fraud," September 6.

Rolnick, Arthur J., and Warren E. Weber. 1983. "New Evidence on the Free Banking Era," *American Economic Review*, vol. 73, no. 5, December, pp. 1080-1091.

Schuman, Evan. 2007. "Stolen TJX Data Used in $8M Scheme before Breach Discovery," *eWeek*, March 21, *www.eweek.com/print_article2/0,1217,a=203568,00.asp.*

Shostack, Adam, and Paul Syverson. 2004. "What Price Privacy?" *Economics of Information Security*, Springer.

Silver, Caleb. 2005. "LexisNexis Acknowledges More ID Theft," CNNMoney.com, June 2, *http://money.cnn.com/2005/04/12/technology/personaltech/lexis/.*

Sweeney, Latanya. 2004. "SOS Social Security Number Watch," The Carnegie Mellon Data Privacy Lab, Spring, *http://privacy.cs.cmu.edu/dataprivacy/projects/ssnwatch/index.html#overview.*

Synovate. 2007. "Federal Trade Comission–2006 Identity Theft Survey Report," November, p. 9, *www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf*

Turner, Dean, Stephen Entwisle, and Eric Johnson, eds. 2007. "Symantec Internet Security Threat Report, Trends for January-June 07," Symantec Security Response, September. *www.symantec.com/content/en/us/about/media/ISTRXII_Main.pdf.*

United States. Census Bureau. 2007. "Income, Poverty and Health Insurance Coverage in the United States: 2006," August.

United States. Securities and Exchange Commission. 2007. *Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934*, The TJX Companies, Inc., March 28, pp. 7-10, *www.sec.gov/Archives/edgar/data/109198/000095013507001906/b64407tje10vk.htm.*

Varian, Hal. 2004. "System Reliability and Free Riding," *Mimeo*, November 30.

Verisign, Inc. 2007. "Critical Alerts," February 9, *www.verisign.com/support/alerts/ua-alerts/040713.html.*

Weber, Harry R. 2005. "ChoicePoint Was Victim of ID Theft in '02," *The Seattle Times*, March 3, *http://archives.seattletimes.nwsource.com/cgi-bin/texis.cgi/web/vortex/display?slug=choicepoint03&date=20050303&query=choicepoint.*

Wolfe, Daniel. 2007. "New Phishing Kits Ease Way for Amateurs," *American Banker*, vol. 172, no. 130, July 9.

_____. 2007. "Security Watch," *American Banker*, vol. 172, no. 162, August 22.

_____. 2007. "94M Accounts in Breach?" *American Banker*, vol. 172, no. 206, October 25.