Data security, privacy, and identity theft: The economics behind the policy debates

William Roberds and Stacey L. Schreft

Introduction and summary

A byproduct of improved information technology has been a loss of privacy. Personal information that was once confined to dusty archives can now be readily obtained from proprietary data services, or it may be freely available (and, as Facebook users know, often voluntarily provided and accessible) through the Internet. While the increased collection and dissemination of personal data have undoubtedly provided economic benefits, they have also diminished people's sense of privacy and, in some cases, given rise to new types of crime.

Is this loss of privacy good or bad? Press accounts repeatedly argue the latter: Too much data are being collected in ways that are too easy for criminals to access.[1] But in a thought-provoking essay, Swire (2003) argues that a meaningful answer to this question requires some notion of *efficient confidentiality* of personal data—that is, of a degree of privacy that properly balances the costs and benefits of our newfound loss of anonymity. In this article, we explore the concept of efficient confidentiality, using some ideas from economic theory.

Loss of privacy: The costs are large and easy to find

The most dramatic consequence of the increased availability of personal information has been the emergence of a new form of payment fraud, *identity theft*. The 1998 U.S. Identity Theft and Assumption Deterrence Act (ITADA) defines identity theft 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. Traditional varieties of identity theft, such as check forgery, have long flourished, but over the last decade, identity theft has become a major category of crime and a significant policy issue.[2]

Identity theft takes many guises, but it is divided into two general categories: *existing account fraud* and *new account fraud*. Existing account fraud occurs when a thief uses an existing credit card or similar account information to illicitly obtain money or goods. New account fraud (traditionally) occurs when a thief makes use of another individual's personal information to open one or more new accounts in the victim's name. Both types of identity theft depend on easy access to other people's data.

Today, identity theft is big business. A study conducted by the Federal Trade Commission (FTC), encompassing both new account fraud and existing account fraud, indicates that in 2006 identity thieves stole about $49.3 billion from U.S. consumers.[3] When the time and out-of-pocket costs incurred to resolve the crime are added in, identity theft cost U.S. consumers $61 billion in 2006 (Schreft, 2007). Even this is a conservative estimate, however, as it omits certain categories of identity theft and some types of costs that are not generally known to consumers. For example, an increasingly prevalent type of identity theft is *fictitious* or *synthetic identity fraud*, in which a thief combines information taken from a variety of sources to open accounts in the name of a new fictitious identity (Cheney, 2005; and Coggeshall, 2007). There is no single victim, in contrast to traditional types of identity theft, but retailers and ultimately consumers end up bearing the cost.

Much of the data used in identity theft is obtained through low-tech channels. In consumer surveys,

William Roberds is a research economist and policy advisor in the Research Department at the Federal Reserve Bank of Atlanta. Stacey L. Schreft is a director of investment strategy at The Mutual Fund Research Center LLC. The views expressed in this article are not necessarily those of the Federal Reserve Bank of Atlanta or The Mutual Fund Research Center LLC.

victims who know how their identifying information was stolen commonly attribute identity theft to stolen wallets or mail or to personal acquaintance with the identity thief (Kim, 2008). In these same surveys, however, the large majority of identity theft victims are unable to pinpoint how the thief obtained their data. Available evidence suggests that much of these data are obtained through illicit access (called "breaches") of commercial or government databases.

Statistics on data breaches are available from information security websites, such as Attrition.org and the Identity Theft Resource Center (www.idtheftcenter.org). Certainly data breaches are numerous and increasing: Attrition.org lists 326 reported data breach "incidents" for 2007, leading to the compromise of 162 million records of personal data, as compared with 11 reported incidents and 6 million compromised records in 2003.[4] These numbers must be placed in perspective. A data breach does not necessarily lead to identity theft, and one reason for the upsurge in reported breaches is the spread of state laws that require consumer notification when a data breach occurs (Anderson, Durbin, and Salinger, 2008). Nevertheless, there is widespread recognition that data breaches promote identity theft. A strong demonstration of this can be found in the August 2008 indictment of an 11-person, global identity theft ring, responsible for the theft of 41 million credit card and debit card numbers, as well as hundreds of millions of dollars in fraud losses.[5]

The benefits of loss of privacy: More subtle, but substantial

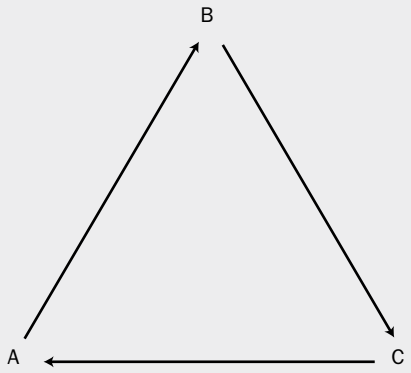
If identity theft costs the U.S. economy so much, are there offsetting benefits? To try and make sense of this question, we will employ a branch of economics known as *monetary theory.* Broadly speaking, monetary theory seeks to understand how transactions are structured within an economy.

The classic model of monetary theory was proposed by Knut Wicksell (1935). Wicksell's model economy is depicted in figure 1 and consists of only three individuals: Andy, Bob, and Clyde (A, B, and C, for short). Andy can produce a good valued by Bob, Bob can produce a good valued by Clyde, and Clyde can produce a good valued by Andy. The point of Wicksell's model is that in real-world economies, transactions typically happen between people who cannot deal through simple barter. For example, when Andy and Bob meet, Bob would like to purchase Andy's good, but the good that Bob has available to trade is only valued by Clyde. How should exchange proceed?

One way to solve this problem is through the use of cash. Suppose that A and B meet on every Monday,

FIGURE 1

Wicksell triangle



Note: See the text for further details.
Source: Wicksell (1935).

B and C meet on every Wednesday, and A and C on Fridays. Then if everyone agrees that the goods they exchange are each worth $1, the economy can function perfectly well with a "money supply" of two dollar bills.[6] For example, Bob sells his good to Clyde on every Wednesday, earning a dollar that he uses to buy Andy's good the following Monday. Andy uses this dollar to buy a good from Clyde every Friday, and so on. This "Wicksell triangle" shows how cash can function as a sort of recordkeeping system for transactions within an economy; every dollar that someone spends is proof of an earlier sale by the same person.[7]

Cash has some well-known limitations, however—some of which appear even in the context of this simple model. For example, if Clyde gets sick or otherwise fails to show up one Wednesday, then Bob will have no money with which to make next Monday's purchase. In practice, cash has other drawbacks, including risk of counterfeit or theft, the inconvenience of finding an automated teller machine (ATM), limited usefulness in telephone and Internet transactions, and the fact that it does not pay interest.

The alternative to cash is credit. In Wicksell's model economy, cash would not be needed if A, B, and C could get together and agree that each individual would receive a good of their preferred type, so long as they had provided a good to someone else the previous week. That way, if an individual occasionally was unable to sell his good during one week, he could still purchase goods on the expectation that he would resume sales the following week. The value of this additional exchange of goods, beyond what would be possible if all transactions were only in cash, is known as a *credit benefit*.

Paying by credit has other advantages, which are the "mirror image" of the disadvantages of cash: fewer trips to the bank, less liability in case of theft, ease in transactions at a distance, and the reduced need to carry non-interest-bearing cash.[8]

Any estimate of the total credit benefit in an economy is somewhat speculative, since it involves the comparison of the value of exchange in an *actual* economy to the value of exchange in a *hypothetical* economy where only cash is available for most transactions.[9] For a developed economy such as that of the U.S., however, this benefit is almost certainly quite large. For example, in 2006 (the year of the FTC identity theft survey), U.S. residents made about $3 trillion in purchases, using credit and debit cards.[10] If the credit benefit of these transactions alone (ignoring other types of credit transactions) amounted to, say, just 5 percent of their total value, the resulting benefit to the overall economy would be $150 billion—more than enough to outweigh the estimated costs of identity theft.

In the rest of this article, we will argue that some loss of privacy is central to the provision of this credit benefit.

Identity: Real and transactional

In Wicksell's model economy, there's no chance of identity theft. Andy, Bob, and Clyde are well known to one another, and as long as one of their mutual friends (say, Dave) can keep a tally of who's provided a good to whom, it would be easy to maintain a credit-based system of exchange. This system would be self-enforcing, since any shirking by one party would quickly be noted by Dave and immediately become apparent to the other parties.[11] Such informal credit systems are common among friends and families, in primitive societies, and in other settings with limited social interactions.

But most transactions in today's economy are either between 1) parties who are total strangers, and/or 2) parties who feel no particular sense of obligation toward one another. Credit in such situations requires some system to control two types of risk. The first type of risk is *credit risk*—the risk that the purchaser may not repay the debt incurred. Overcoming credit risk requires a way to keep track of "credit histories," that is, a way to restrict the use of credit to people who habitually pay their bills. The second type of risk is *fraud risk*—the risk of deception by the purchaser. Overcoming fraud risk requires a way to associate transactors with credit histories: For example, I may have a spotless credit record, but somehow that information has to be conveyed to the grocery store before I'm allowed to leave the store with a bag of groceries. To be effective, both types of services require the accumulation, storage, and distribution of large amounts of personal data. But the data required by the second service concern a person's *identity*, and are bound to be of a more confidential and controversial nature.[12]

"Identity" in general refers to all the distinguishing attributes of an individual—potentially a very long list. The term *personal identifying data* (PID) is used to describe some portion of a person's identity—name, birth date, Social Security number, etc.—that is readily observable by others. In order to distinguish individuals, the credit bureaus, credit card companies, data brokers, and other parties in the credit industry have compiled large databases of PID. These subsets of a person's "real" identity that are stored by these parties and used in transacting can be thought of as *transactional identities* (Schreft, 2007). Once the relevant data have been verified, a person's transactional identity may be augmented by the creation of new, synthetic data unique to that person, such as a credit card number, PIN (personal identification number), and so on (Kahn and Roberds, 2008).

A typical credit transaction—say, a purchase of a bag of groceries, using a credit or debit card—can be thought of as a merchant exchanging goods in return for two essential pieces of payment information corresponding to the types of risk described previously: 1) that the purchaser, based on his credit history, is likely to pay his bill[13] and 2) that the purchaser's transactional identity is genuine so that the consumer is not a fraudster.

Transactional identities as club goods

All credit-based payments require systems for processing valuable information. We can think of this information (credit histories and transactional identities) as economic *goods*, or items having value in exchange. These goods have value, since they facilitate the exchange of other goods (say, groceries) that people want to consume. Electronic versions of payment data, once amassed, can be stored at a few locations and then shared among payment system participants at very low cost. The data used in credit-based transactions meet Varian's (1998) description of a *digital good*, a good that can be stored and transferred in digital form.

Digital goods are also *nonrival* goods, meaning that they are not diminished by successive use. This distinguishes them from *rival* goods, such as cars and cornflakes; one individual's consumption of a rival good diminishes or eliminates the possibility of another person consuming it. Other examples of digital (and also nonrival) goods are given by the electronic information that is incorporated into broadcast and

cable television, computer programming, or recorded music and video: For instance, my consumption of an episode of *American Idol* does not diminish another's enjoyment of the same episode. The same holds true with payment data, including transactional identities: The fact that Wal-Mart knows that I am not a fraudster does not diminish the value of the same information to Home Depot.

Nonrival goods are classified as *club goods* or *public goods*. A club good is an *excludable* nonrival good—that is, one for which a group or individual can be excluded from consuming (for example, cable TV programming).[14] A public good is a *nonexcludable* nonrival good—that is, one for which access cannot be limited (for example, national defense or clean air). The club good classification is more appropriate for payment information, since access to this information can be controlled (to a greater or lesser degree).

The "nonrivalness" of electronic payment information is a tremendous source of economic efficiency. Turning the clock back several decades, in any retail situation involving credit, a merchant had to independently come by the information needed to assess a customer's creditworthiness. The high cost of this information meant that credit was impractical in many situations, for example, during travel or for small transactions. The development of the credit industry (the large databases of credit histories and transactional identities, credit and debit cards, electronic authorization procedures, and antifraud technologies) has meant that merchants can take advantage of economies of scale in managing this information, and has spread the costs of information management over a larger group of merchants (and, ultimately, consumers).[15] This has, in turn, increased the credit benefit available to society as a whole.

Of course, the transformation of payment information into a nonrival good has not occurred in isolation. All kinds of data (music, video, maps, encyclopedias, and celebrity gossip) have been widely digitized, and thanks to the essentially nonrival nature of digital goods, they are rapidly accumulated and widely disseminated.

The dark side of nonrivalness

A central feature of any digital good is its quality. Recorded music or video, for example, is useless if the original is garbled. A potentially interesting website may seem less so if it is known to harbor computer viruses. Quality is especially critical for payment data because people using a payment system expect it to work flawlessly virtually 100 percent of the time. Contamination of a payment system's data through even a few errors or instances of fraud can quickly erode its value.

A "dark side" of the efficient production of payment information is that it can compromise quality; that is, it can facilitate fraudulent activity as well as legitimate use. Once a fraudster has assumed another person's transactional identity (through either new or existing account fraud), the fraudster becomes an apparently legitimate participant in one or more payment systems and, by extension, a legitimate participant in the eyes of many participants in those systems. This vulnerability means that payment data, as an economic good, will only have value in the presence of the complementary good "data integrity," which is the quality and reliability of the data incorporated into the payment system (Braun et al., 2008).[16] Data integrity, like the underlying payment data, is a nonrival (club) good: The assurance that a payment information database is secure against data breaches is not diminished by successive use.

Another widely recognized drawback of modern payment arrangements stems from the more difficult to measure, but nonetheless important, consequences of diminished privacy. That is, the digitization of personal data contained in transactional identities has made these data available to many more people than ever before, often with negative consequences. These may take the form of intangible, but undeniable, costs in terms of people's loss of a "sense of space" about their personal lives. Or, for victims of identity theft, these costs may assume a more concrete form, through harassment by bill collectors, misplaced civil lawsuits, or even criminal investigations.

Many current payments and credit practices can be interpreted as attempts to partly restore the sense of privacy that may have existed in earlier times. When someone makes a purchase with a credit card, for example, that purchaser must effectively reveal some information to the merchant concerning his transactional identity—at least in the form of a relatively anonymous credit card number. This "surrender" of information represents a compromise between the merchant's need to identify the purchaser and the purchaser's desire to preserve his own privacy. Ideally, the merchant obtains enough information about the purchaser to determine that the transaction is legitimate, but no more. Consumers themselves have also undertaken forceful actions to safeguard their privacy, removing their names from public directories and mailboxes, installing paper shredders in their homes, and only giving out personal information to the most trusted parties.

Ironically, these very attempts to restore privacy may have contributed to the rise of identity theft, according to LoPucki (2003). LoPucki points out that in earlier times, individuals' access to credit often depended

on their public persona, that is, on their standing within a local community or circle of business associates. Those seeking access to credit had to sacrifice much of their privacy (say, by socializing with their neighbors on a regular basis or joining civic organizations) in order to gain a reputation as an upstanding and creditworthy individual. Modern information technology, by enabling "instant credit" between relatively anonymous parties, has reduced the need for a public persona, but it has also multiplied the potential for fraud.

Efficient confidentiality: Beyond supply and demand

Using the ideas outlined thus far, we can now look at the issue of efficient confidentiality. The term *confidentiality* has a specific meaning in our context, which is the likelihood that a person's transactional identity will not be observed by miscreants and put to inappropriate use. A person's confidentiality can be thought of an economic good, whose provision in the marketplace depends on two other economic goods: 1) the amount of PID incorporated into that person's transactional identity and 2) the level of security for these data, or the degree of data integrity applied to the person's transactional identity. An increase in the second good always improves confidentiality. An increase in the first good can improve confidentiality, up to a point. The more data that are collected (all else being equal), the more precise the identification of individuals is, and hence, the greater the availability of credit-based payment is throughout the economy. But increasing the amount of PID collected (again, all else being equal) reduces privacy and can also amplify the negative consequences that occur when such data are misused, eroding confidentiality.

How should we know if these two goods (data collection and data security) are being efficiently provided? Textbook economic theory says that for many goods, it is (conceptually, at least) easy to describe how that good can be efficiently provided: An efficient market exists for a good when its supply curve intersects with its demand curve. The demand curve for a good, in turn, is given by its marginal benefit to buyers, and the supply curve is determined by sellers' marginal cost of producing that good. In a competitive industry, if the price of a good is above (below) its marginal cost, producers enter (leave) the industry until efficiency prevails.

Unfortunately this familiar model doesn't work for digital goods, since their marginal cost is practically zero. Instead, a more typical pattern for digital goods is for there to be competition among a few large producers, which are able to take advantage of the extensive economies of scale in these goods' production (think of the computer software and entertainment industries). Prices remain above marginal costs, so as to defray the costs of production.

We see the same pattern in the construction of transactional identities by a relatively small number of large players such as credit bureaus, credit card networks, and card issuing banks.[17] Through the accumulation of large amounts of PID, these organizations attempt to meet the demand for transactional identities that exists in the market economy. Just as with other digital goods, such as computer software and recorded video, it is hard to know whether these data are being efficiently collected and priced.[18]

The situation is different when we turn to the issue of data integrity. Because payment data are only useful if they are communicated (in some form), these data must be touched by a large number of hands to be of any value. A real-world list of such hands would include consumers, merchants, credit bureaus, banks, and payment processors. In other words, efficient production of data integrity, a club good, requires the cooperative efforts of a large number of "club members."

Large clubs often promote efficiency because they allow for economies of scale in the production of a good. But within large clubs, conflicts of interest can arise as to the amount of the good that should be provided. This is especially true for goods such as data integrity, for which the "weakest link" or "flood control" model of a nonrival good is often applicable (Hirshleifer, 1983).

For a weakest link good, the total amount of the good provided to the club is equal to the lowest amount of the good supplied by a club member (the weakest link in a chain, or the lowest levee in a flood control system). The idea of a weakest link is consistent with many press accounts of identity theft, in which a data breach at a single retailer or payment processor leads to widespread fraud. There is a natural tendency to supply an inefficiently small amount of a weakest link good (Varian, 2004), which can arise from the following conflict: A club member with relatively little at stake will tend to put less effort into providing the club good than a club member with a lot at stake. This tension is present in many situations involving data security (Anderson and Moore, 2006).

Recent changes in the payments industry's security practices can be seen as a response to this problem. For example, a set of industry-wide data security standards—the PCI (Payment Card Industry) standards (www.pcisecuritystandards.org)—has been created as a way of strengthening the weakest links in the data security chain. Another development along these

lines has been the increasingly common practice of merchants quickly disposing of payment data, rather than storing it for an extended period of time.[19]

An additional source of inefficiency comes from externalities (also called spillovers) across data security practices. An *externality* occurs when the consumption or production of a good by one party affects another's, conferring benefits or costs on the other party. A negative externality results when a party does not take into account the full cost of his action to others.

In the context of data security, the potential for negative externalities exists for at least two reasons. First, as noted previously, payment data often passes through many hands, so it is difficult to determine how an identity thief was able to access the necessary data. Second, under current U.S. and Canadian laws, recovering the costs of a data breach through the courts can be difficult (Schreft, 2007; and Chandler, 2008). Either way, if payment data are stolen from one party and used to commit identity theft with costly consequences for another, the first party may not expect to pay the full costs of the breach. Taken together, these complications suggest that there are obstacles to the efficient provision of data integrity in the marketplace. Because payment system participants may not fully take into account all of the costs associated with their security practices, this can lead to underprovision of data security. This would, in turn, imply an inefficiently low level of confidentiality in the marketplace, even if the market is collecting the "right" amount of PID.

In Roberds and Schreft (2008), we present a model that shows how this inefficiency could be exacerbated by the interaction between PID collection and data security. If some payment systems are not adequately securing their data and other payment systems are alerted to this, then each system's best safeguard against identity theft may be to increase the amount of PID it uses for transactional identities. Under these circumstances, gathering more PID can reduce fraud, but doing this is inefficient because it further reduces confidentiality.

Roles for regulation

The previous discussion points to a role for public policy. If the markets for information on transactional identities are providing inefficiently low levels of confidentiality, there may be ways for well-designed policies to improve on market outcomes.

One policy implication that is *not* supported is government entry into the markets for payment information. As with other types of club goods, the excludability of payment information provides a profit incentive to motivate ongoing improvements in efficiency. But the production of club goods is rarely a straightforward business, and it is usually subject to extensive policy interventions. Electronic entertainment products, computer software, and various types of Internet content, to name just three examples, are frequent subjects of public controversy, legislation, regulation, and litigation.

This same general pattern is found in the markets for payment information. Various pieces of legislation and regulatory efforts have sought to address the "weakest link" and "spillover" problems identified before, but have stopped short of trying to micromanage industry practices. For example, the Fair and Accurate Credit Transactions Act of 2003 (commonly known as the FACT Act) seeks to increase the industry standards for minimally acceptable security practices. The FACT Act requires banks and other creditors to develop procedures to respond to account activity that could reasonably be interpreted as evidence of identity theft ("red flags"), but does not specify the details of how this should be done.[20]

In the same vein, a number of state laws now require that consumers be notified whenever their data are breached. One motivation for this requirement is to enable quicker detection of identity theft by consumers. An equally important purpose for this requirement, though, may be to motivate better security practices by increasing the costs of a data breach (in terms of both dollars and reputation). A number of states have taken another tack, which is to allow consumers to limit or "freeze" access to their credit reports, that is, to limit access to information on their transactional identities.

A concern with this type of regulation is the cost of compliance. Since securing data is costly, perfect confidentiality of personal data cannot be an efficient outcome, and should not be a goal of sensible regulation. As outlined in this article, some amount of identity theft is inevitable given modern information technology. Eliminating identity theft entirely would not be possible without eliminating the efficient sharing of information at the heart of our modern credit and payment systems.

Public goods

Government intervention is traditionally viewed as beneficial when it yields public goods. One such good is "public security," as is provided by the criminal justice system. The ITADA and various state laws have sought to discourage identity theft by imposing severe criminal penalties—a form of deterrence not available to the private sector.

The nature of identity theft puts limits on the effectiveness of criminal sanctions, however. By stealing

someone else's payment data, an identity thief gains that person's access to credit in largely anonymous situations, such as in purchases over the Internet. This same anonymity that benefits legitimate purchasers (in terms of access to credit with increased confidentiality) makes criminal prosecution of identity theft impossible in many cases—as when the identity thief is located in a different country from that of the victim.

Another noteworthy public good in this context is that of overall "confidence" in credit and payment systems. As discussed previously, people do not like to use payment systems without something close to 100 percent reliability. If incidences of identity theft and data breaches were to become sufficiently common, the result could be a loss of this public good—that is, a loss of confidence not only in the directly affected parties, but in credit-based payment more generally (Braun et al., 2008). One rationale for recent regulatory actions in the payments area is that, apart from the effects of any specific provisions, these laws and regulations demonstrate governments' commitment to maintain a reasonable standard for confidentiality of payment information.

Conclusion

In this article, we have looked at the issue of confidentiality of personal information from the standpoint of economic theory. Some loss of privacy is necessary for the credit benefit, which is a key advantage of modern payment systems. By consolidating personal information into transactional identities, information technology now allows people to enjoy this credit benefit in circumstances that would have been unthinkable a generation ago.

The sharing of information on transactional identities is vital to the operation of these payment systems. However, this information sharing can facilitate fraud in the form of identity theft. Information sharing can also create conflicts of interest that may not be easily resolved through the operation of the marketplace. Thoughtful public policy should be aimed at resolving these conflicts and providing public goods. The ultimate goal of regulation should not be absolute privacy of consumers or complete suppression of identity theft, but instead the promotion of efficient confidentiality of personal information.

NOTES

[1]See, for example, Stone (2007), Swartz and Acohido (2007), Caruso (2007), and Dow Jones and Company Inc. (2008b).

[2]There are no time-series data on identity theft rates, but one measure of the extent of the problem is the how often the term "identity theft" shows up in press reports. Anderson, Durbin, and Salinger (2008) report 30 mentions of "identity theft" in U.S. newspapers in 1995; 2,000 in 2000; and 12,000 in 2005.

[3]This estimate is from a survey of consumers reported in Synovate (2007); for extensive discussions of this survey, see Schreft (2007) and Anderson, Durbin, and Salinger (2008).

[4]Of course not all data breaches are publicized, so these numbers are probably underestimated.

[5]See, for example, Stone (2008). For other recent data breach incidents, see Braun et al. (2008).

[6]If we increase "money velocity" by changing the order of transactions (say A and C meet on Wednesdays and B and C on Fridays), then a money supply of one dollar bill will be sufficient.

[7]Beginning with Kiyotaki and Wright (1989), this role for cash has been extensively developed in "search" models of money; Wright (2008) surveys this literature.

[8]For a detailed comparison of the costs of cash versus other forms of payments in certain retail settings, see Garcia-Swartz, Hahn, and Layne-Farrar (2006).

[9]Even for the simple Wicksell model, calculation of a credit benefit can be a challenging exercise. Taub (1994) shows that for this model, people can sometimes do just as well by keeping hoards of cash. However, Kocherlakota (1998) shows that in general an economy's credit benefit will be a positive number.

[10]Bank for International Settlements, Committee on Payment and Settlement Systems of the Group of Ten Countries (2008). Use of a debit card can result in a credit benefit if the card is attached to a bank account with an overdraft privilege or line of credit.

[11]In some simple economies like Wicksell's, Araujo (2004) shows that Dave may not be needed; mutual confidence that others will honor their obligations is enough to sustain credit-based exchange. Kahn and Roberds (2009) discuss how Wicksell's model can be used to analyze various types of payment systems.

[12]Credit risk and fraud risk are often difficult to separate. For example, if a person applies for a credit card, runs up a bill, and then never makes a payment, then it may be hard to tell whether the person meant to commit fraud or just wasn't able to pay. Or someone may refuse to pay for his credit card purchase, claiming the transaction was fraudulent; this practice is sometimes known as "friendly fraud." Nonetheless, it is useful to conceptually distinguish between these two types of risk.

[13]There is an element of credit even with many transactions that are thought of as "instantaneous" (for example, debit card or Internet banking payments), since these do not settle instantaneously. In many card transactions, the card issuer assumes the "credit risk" that the card payment will not be repaid by the cardholder.

[14]For example, one can imagine all viewers of ESPN (Entertainment and Sports Programming Network) as members of a club who pay membership fees to the club through their monthly cable or satellite television bill.

[15]An *economy of scale* occurs when an increase in the production of a good lowers its average cost. In our context, the increased accumulation and distribution of payment information have lowered the average cost of accessing such information.

[16]A *complementary good* is defined as a good that is consumed with a second good, for which an increase in the demand for the first good results in an increase in demand for the second. For example, cars and gasoline are complementary goods.

[17]The structure of this industry has been changed by the emergence of data brokers (legal and illegal) and other entities that compile and trade PID obtained from other sources (Schreft, 2007).

[18]For example, one could interpret the famous antitrust case brought by Wal-Mart and other retailers against Visa and MasterCard, settled in 2003 for $3 billion, as a dispute over the efficient pricing of access to payment information, including the validity of cardholders' transactional identities.

[19]This practice of merchants quickly disposing of payment data has been incorporated into the PCI standards; the practice came about in part because of legislation discussed later in this article. See, for example, Dow Jones and Company Inc. (2008a).

[20]More specific guidelines were jointly issued by six federal regulatory agencies, including the Federal Reserve System, in 2007. See Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, and Federal Trade Commission (2007).

REFERENCES

Anderson, K. B., E. Durbin, and M. A. Salinger, 2008, "Identity theft," *Journal of Economic Perspectives*, Vol. 22, No. 2, Spring, pp. 171–192.

Anderson, R., and T. Moore, 2006, "The economics of information security," *Science*, Vol. 314, No. 5799, October 27, pp. 610–613.

Araujo, L., 2004, "Social norms and money," *Journal of Monetary Economics*, Vol. 51, No. 2, pp. 241–256.

Bank for International Settlements, Committee on Payment and Settlement Systems of the Group of Ten Countries, 2008, *Statistics on Payment and Settlement Systems in Selected Countries*, Basel, Switzerland: Bank for International Settlements, March.

Braun, M., J. McAndrews, W. Roberds, and R. Sullivan, 2008, "Understanding risk management in emerging retail payments," *Economic Policy Review*, Federal Reserve Bank of New York, Vol. 14, No. 2, September, pp. 137–159.

Caruso, D., 2007, "Securing very important data: Your own," *New York Times*, October 7, available at www.nytimes.com/2007/10/07/technology/07frame.html.

Chandler, J. A., 2008, "Negligence liability for breaches of data security," *Banking and Finance Law Review*, Vol. 23, No. 2, pp. 223–273.

Cheney, J. S., 2005, "Identity theft: Do definitions still matter?," Federal Reserve Bank of Philadelphia, Payment Cards Center, discussion paper, No. 05-10, August.

Coggeshall, S., 2007, "ID theft knows no boundaries," *E-Commerce Times*, April 13, available at www.ecommercetimes.com/story/56864.html.

Dow Jones and Company Inc., 2008a, "New payment card data mantra is 'Don't need it, don't store it,' " *Wall Street Journal*, September 16, available by subscription at http://online.wsj.com/article/SB122153790800641877.html.

_____, 2008b, "Data breaches surpass 2007 level, but businesses rarely are penalized," *Wall Street Journal*, September 9, available by subscription at http://online.wsj.com/article/SB122093405633914081.html.

Garcia-Swartz, D. D., R. W. Hahn, and A. Layne-Farrar, 2006, "The move toward a cashless society: A closer look at payment instrument economics," *Review of Network Economics*, Vol. 5, No. 2, June, pp. 175–198.

Hirshleifer, J., 1983, "From weakest link to best shot: The voluntary provision of public goods," *Public Choice*, Vol. 41, No. 3, January, pp. 371–386.

Kahn, C. M., and W. Roberds, 2009, "Why pay? An introduction to payments economics," *Journal of Financial Intermediation*, Vol. 18, No. 1, January, pp. 1–23.

_____, 2008, "Credit and identity theft," *Journal of Monetary Economics*, Vol. 55, No. 2, March, pp. 251–264.

Kim, R., 2008, *2008 Identity Fraud Survey Report (Consumer Version): How Consumers Can Protect Themselves*, Pleasanton, CA: Javelin Strategy and Research, February, available at www.javelinstrategy.com/research/all.

Kiyotaki, N., and R. Wright, 1989, "On money as a medium of exchange," *Journal of Political Economy*, Vol. 97, No. 4, August, pp. 927–954.

Kocherlakota, N. R., 1998, "Money is memory," *Journal of Economic Theory*, Vol. 81, No. 2, August, pp. 232–251.

LoPucki, L., 2003, "Did privacy cause identity theft?," *Hastings Law Journal*, Vol. 54, No. 4, April, pp. 1277–1298.

Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, National Credit Union Administration, and Federal Trade Commission, 2007, "Identity theft red flags and address discrepancies under the Fair and Accurate Credit Transactions Act of 2003," *Federal Register*, Vol. 72, No. 217, November 9, p. 63718, available at www.gpoaccess.gov/fr/.

Roberds, W., and S. L. Schreft, 2008, "Data breaches and identity theft," Federal Reserve Bank of Atlanta, working paper, No. 2008-22, September.

Schreft, S. L., 2007, "Risks of identity theft: Can the market protect the payment system?," *Economic Review*, Federal Reserve Bank of Kansas City, Fourth Quarter, pp. 5–40.

Stone, B., 2008, "11 charged in theft of 41 million card numbers," *New York Times*, August 5, p. C1, available at www.nytimes.com/2008/08/06/business/06theft.html.

_____, 2007, "To fight identity theft, a call for banks to disclose all incidents," *New York Times*, March 21, available at www.nytimes.com/2007/03/21/business/21identity.html.

Swartz, J., and B. Acohido, 2007, "Who's guarding your data in the cybervault? ChoicePoint redeemed itself but not all brokers as careful," *USA Today*, April 2, p. 1B, available at www.usatoday.com/educate/college/careers/Car_foc/4-02-07.htm.

Swire, P. P., 2003, "Efficient confidentiality for privacy, security, and confidential business information," in *Brookings–Wharton Papers on Financial Services: 2003*, Richard Herring and Robert E. Litan (eds.), Washington, DC: Brookings Institution Press, pp. 273–310.

Synovate, 2007, *Federal Trade Commission—2006 Identity Theft Report*, McLean, VA, available at www.ftc.gov/os/2007/11/SynovateFinalReportIDTheft2006.pdf.

Taub, B., 1994, "Currency and credit are equivalent mechanisms," *International Economic Review*, Vol. 35, No. 4, November, pp. 921–956.

Varian, H. R., 2004, "System reliability and free riding," University of California, Berkeley, report, November 30, available at http://people.ischool.berkeley.edu/~hal/Papers/2004/reliability.

_____, 1998, "Markets for information goods," University of California, Berkeley, report, October 16, available at http://people.ischool.berkeley.edu/~hal/Papers/japan/.

Wicksell, K., 1935, *Money*, Vol. 2, *Lectures on Political Economy*, New York: Macmillan.

Wright, R., 2008, "Search-and-matching models of monetary exchange," in *The New Palgrave Dictionary of Economics*, S. N. Durlauf and L. E. Blume (eds.), 2nd ed., New York: Palgrave Macmillan.