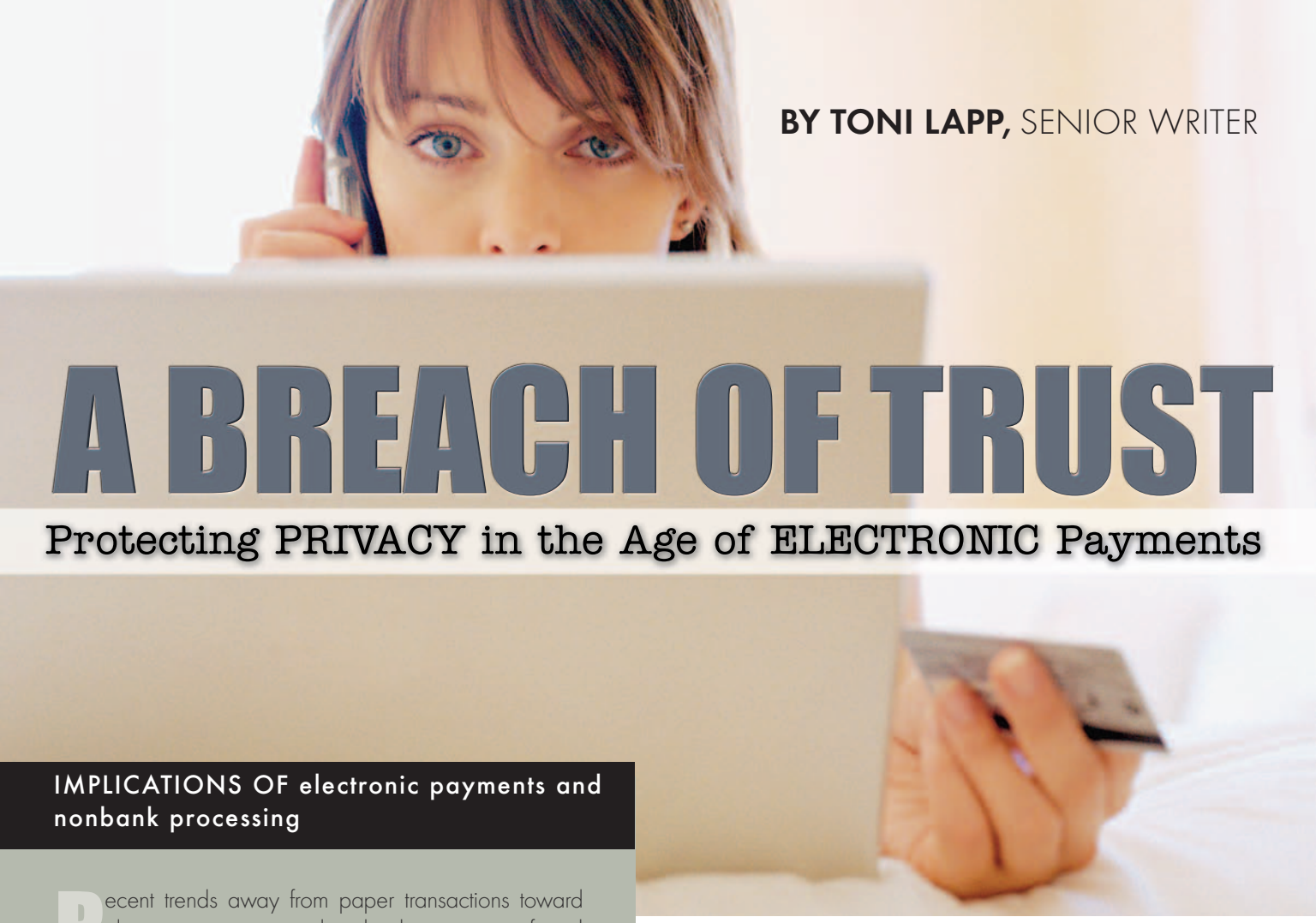


BY TONI LAPP, SENIOR WRITER

A BREACH OF TRUST

Protecting PRIVACY in the Age of ELECTRONIC Payments

IMPLICATIONS OF electronic payments and nonbank processing

Recent trends away from paper transactions toward electronic payments and nonbank processing of retail payments are brought about by the desire to increase efficiency by exploiting economies of scale in payment processing, argues **Senior Economist Richard Sullivan in his working paper "The Supervisory Framework Surrounding Nonbank Participation in the U.S. Retail Payments System: An Overview."**

There are many implications to the increased reliance on electronic payment networks. The scale of operations and the interdependencies among elements of the network increase the potential for widespread disruptions.

Sullivan's paper describes the supervisory structure over nonbank participants in the U.S. payments system and reviews how policy tools such as standards setting, disclosure, clarifying legal responsibilities, and supervision can each play a role in improving control of payments system risk.

TO ACCESS A PDF VERSION of the full document, published by the Payments System Research Department of the Federal Reserve Bank of Kansas City, go to www.KansasCityFed.org/TEN.

The letter from the retailer was generic but polite, explaining that the company was investigating the theft of customer data that included credit card and debit card numbers. Midway through, the real purpose of the correspondence emerged: to notify the Designer Shoe Warehouse (DSW) customer that her account information was among the data stolen months before.

The same letter was sent to 1.4 million other customers who made purchases with charge cards or checks, including Federal Trade Commission chairwoman Deborah Platt Majoras.

Clearly, no one is exempt from the threat of breached data.

The question of how to protect consumers' privacy has been around for years, long before a number of breaches this year resulted in millions of consumers' personal data being exposed.

When the issue came up in Congress, U.S. financial institutions favored an "opt-out" system that was put into law by the Gramm-Leach-Bliley Act in 1999. In other words, consumers who don't want their personal information to be shared must opt out in writing, a scheme that favors businesses who want to sell their customers' information. The law, known as GLBA, also established that financial institutions have a responsibility to protect "nonpublic" information such as account numbers and Social Security numbers.

As a result, some observers think GLBA has become a double-edged sword. Financial institutions asked for freedom to use the information, and now they have to bear the responsibility to protect it.

According to a recent working paper by Richard Sullivan, senior economist in the Payments System Research Department at the Federal Reserve Bank of Kansas City, data breaches are examples of operational risk in payments. Sullivan's paper discusses risk control in the U.S. retail payments system in light of the proliferation of electronic payments.

So how well are companies doing?

In the first half of 2005, 50 million accounts had been breached in a variety of incidents. More disturbing is that the issue has moved beyond financial institutions and even their vendors, as the DSW case illustrates. The shortcomings of GLBA have been clear in many of these cases; the legislation, as currently written, only applies to financial institutions that deal directly with consumers.

"What's troubling me is a lot of the data that's a target for hackers is your account information; that's where the money is. And more of that information is in a more readily accessible form in financial and nonfinancial institutions as well as at retailers," said Sullivan.

The weakest link

Identity fraud is actually on the decline. A 2005 study by a credit industry consultant found that in a year's time, 9.3 million American adults were victims of identity fraud, a 7.9 percent drop from a study in 2003.

However, the mean cost of each theft increased 12 percent. Thieves are stealing more from their victims. The average out-of-pocket cost to the victim was $652, and the time spent to resolve ensuing problems averaged 28 hours. Clearly, identity fraud is costly, consuming money and time.

Thieves are going where the access is: the Internet. While identity theft in general is declining, attacks on Internet users appear to be increasing, based on a seven-year study by the Financial Crimes Enforcement Network. Reports of suspicious activity tied to Internet or online banking were on the rise by 2002.

A lot of publicity has been given to the

An insider's view of security proposals

Joshua Peirez, senior vice president and associate general counsel at MasterCard International, was at the Federal Reserve Bank of Kansas City recently to address officials involved in supervision, research and operations at the Bank. Peirez, who has testified before Congress on the issue, spoke largely about risk in the payments system in the wake of recent data breaches.

WHAT IS HIS VIEW OF PROPOSED LEGISLATION?

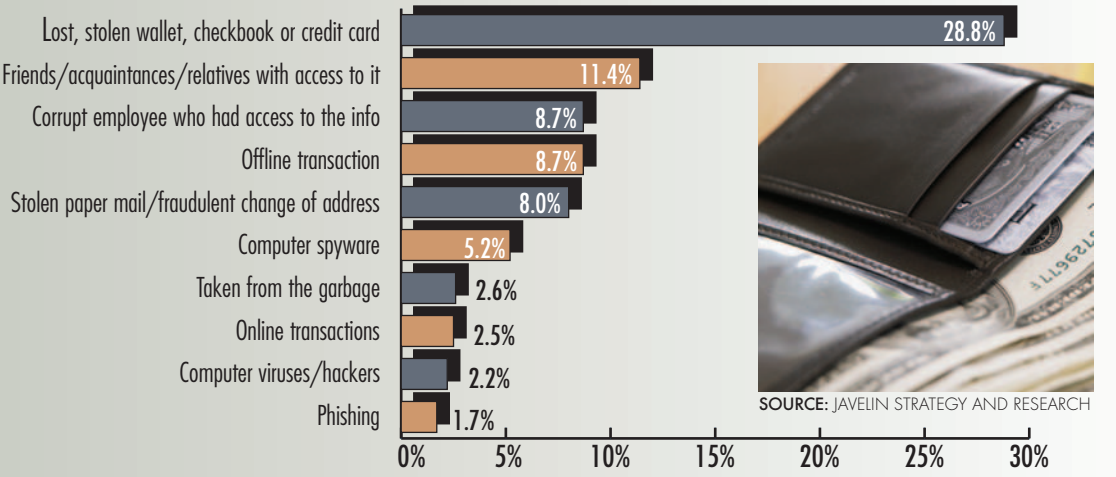
THE PUNISHMENT NEEDS TO MATCH THE CRIME. "It is critical that criminal penalties are increased to fit the magnitude of these crimes and that the crimes themselves are easy for law enforcement and prosecutors to prove," says Peirez.

THE GRAMM-LEACH-BLILEY ACT, with its requirements for storing sensitive data, should be expanded beyond defined "financial institutions," says Peirez. Any entity-retailers, marketers and payments processor that stores, transmits or uses sensitive consumer data also should have clear obligations to safeguard this data.

HAVING A UNIFORM NOTIFICATION LAW that provides consumers with notice both when they reasonably need it and in a way that they can make use of the information makes sense, says Peirez. It is important to work to find the right balance so that consumers are not overnotified or undernotified. It isn't easy to accomplish, but it is important, says Peirez.

Primary Methods of Identity Theft

(From Known-Cause Cases)



SOURCE: JAVELIN STRATEGY AND RESEARCH

risks posed by electronic payment methods; however, most thieves obtained personal information using "offline" methods—billfolds were lost or stolen, acquaintances or family members abused their access or mailboxes were compromised.

That said, a number of means for information to fall into the wrong hands exists in the world of electronic payments. The chart above shows the most common methods criminals use to access sensitive information.

> **"We have little systematic evidence on whether data breaches are occurring more or less in bank or nonbank organizations."**

With the growing complexity of technology and the increasing innovations in payment methods, it's a reasonable public policy question to ask what rules regulators are creating to address changing security risks.

When national media reported earlier this year that 40 million credit cards stored by a technology service provider had been breached, it shed light on the potential for fraud when a customer makes a purchase with a charge card.

After all, such purchases involve a labyrinth of steps during which a weak link can be exploited by a thief.

The company responsible for the breach, CardSystems Solutions Inc., is a payment processor, which acts as an intermediary between merchants and credit card issuers like MasterCard and Visa.

What of the protections mandated by GLBA? The law only applies to financial institutions providing services to consumers.

Because of the need for advanced technology in the era of electronics payments processing, outsourcers such as CardSystems have sprung up in recent years. The danger is that outsourcers add another step in the movement of money, another place in a network for people to tap into.

As the number of outsourcers increases, so will the risk to the payments system.

So who's watching for weak links?

In his paper, Sullivan describes the supervisory structure over providers of technology services to banks, which is administered by a little-known agency named the Federal Financial Institutions Examination Council, or FFIEC. FFIEC comprises members of all the federal agencies responsible for regulation and supervision of U.S. depository institutions, including the Federal Reserve System. The FFIEC assesses risk in providers of technology services to

banks and coordinates examinations of the riskiest providers.

Typically, the team that reviews the firm comprises examiners from member agencies, such as the Federal Reserve, the Federal Deposit Insurance Corporation and the Office of Comptroller of the Currency. This ensures that the firm only undergoes one exam, but that all agencies are kept apprised of developments. This program reduces regulatory burden on a firm and improves supervisory efficiency.

Nonbank providers of payment processing services are part of the supervision program. The FFIEC risk assessment would likely place the largest payments processors in the supervision program, but due to limited information, resources and jurisdiction, only 125 payment processors are supervised, Sullivan notes in his paper.

CardSystems Solutions was one of about 500 payments processors; clearly many of these firms go unsupervised. Whether this poses much risk to payments is uncertain.

"We have little systematic evidence on whether data breaches are occurring more or less in bank or nonbank organizations or among supervised or unsupervised technology service providers," says Sullivan.

Public policy

Who should bear the costs of security breaches? When credit cards are used fraudulently for online purchases, merchants pay for the fraud, not the card issuer. Some argue that this gives little incentive for card issuers to implement anti-fraud measures. Similarly, cardholders may not have incentive to exercise vigilance when they are protected by loss limits.

To protect the payments system, analysts have proposed legal reform and regulation to rationalize liability and responsibility for risk in contracting relationships for payment processing. Lawmakers are considering more severe consequences for mishandling sensitive information.

It is likely that public disclosure will be addressed by future legislation. The CardSystems Solutions breach was discovered by Australian bank officials in late 2004, yet it wasn't reported in the United States until June 2005. Officials have declined to say when the FBI was notified.

What frustrates researchers trying to study the issue is the lack of cold, hard data. Out of millions of data exposures occurring this year, it is unknown how many resulted in actual losses to individuals.

The letter to the DSW customer intimated as much: "We cannot know if your credit card or debit card will or will not be used by the thieves to commit fraud," it said.

Sullivan says getting better information on these crimes should be a priority: "As a society we will have to deal with these things as they come along. You can't fix security problems until you know what they are and how bad they are."

T

COMMENTS/QUESTIONS are welcome and should be sent to teneditors@kc.frb.org.

Modus Operandi

There are a number of methods **the criminally minded can employ ONLINE** to do harm:

1 **SPYWARE:** These are programs that, when installed on a computer, can change settings, display advertising, track Internet behavior and report information back to a central database. Spyware may be installed unintentionally by users, and can be very difficult to remove. This type of breach was responsible for 5.2 percent of cases of identity theft, the single most common online breach.

2 **PHISHING:** In this type of attack, an e-mail that appears to come from a legitimate company (for instance, eBay) is sent to recipients, who are asked to go to a site to update records and verify username and password. The site is actually a place to collect that information and steal identities, money, records and more. Phishing was cited in a recent study in 1.7 percent of identity theft cases.

3 **HACKING:** Many types of malfeasance–computer worms, Trojan horses and more–fall under this moniker. Hackers, a term used to describe criminals who subvert computer security without authorization, were responsible for about 2.5 percent of known cases of identity theft. CardSystems Solutions was victim to hacking.