



Payments Security:

As Strong as the Weakest Link





Each year, millions of Americans fall victim to identity theft because of data breaches. Several economists discuss the payments industry's vulnerability to breaches and also give advice on increasing security.

Imagine receiving your monthly credit card statement and cautiously reviewing it as you do every month. But this time, as your eyes scan down the page, some of the purchases are unfamiliar. An entry for \$532.78 at Barneys New York? Over \$700 spent at NeimanMarcus.com? Your pulse quickens. You never visited these sites! You begin to panic as you realize that someone with extravagant fashion taste has stolen your credit card information. Along with the millions of Americans each year whose identities are stolen, you have been the victim of a data breach. (See the table for a yearly breakdown of exposed information records.)

Several major data breaches occurred in the first half of 2011 alone. In one breach that lasted from February through May, thieves tampered with PIN pads at Michaels Stores across the country. When the company finally discovered the breach, it had to replace 72,000 devices. In another incident, this one made public in April, Sony had to shut down its PlayStation Network when it discovered that personal data had been stolen from more than 77 million accounts. Given the unprecedented magnitude of this pilfered data, consumers and politicians fiercely criticized Sony for failing to disclose the breach until almost a week after learning of the incident.

Data breaches like these are becoming a disturbingly common feature of today's headlines, yet the experts still cannot calculate with any reasonable confidence their ultimate cost. It may be some time yet before it is possible to estimate the full extent of the financial losses from these breaches, as the stolen data work through the criminal supply chains that buy, sell, and use personal information for fraudulent purposes.

Meanwhile, what makes the payments industry vulnerable to fraud? What steps can the industry take to protect your data? Economists may be able to supply some of the answers.

Annual U.S. Data Breaches

Year	Data breaches	Number of records exposed
2007	446	127,717,243
2008	656	35,691,255
2009	498	222,477,043
2010	662	16,167,542
Q1 2011	112	5,460,925

Source: Identity Theft Resource Center

The externalities of personal data collection

According to Will Roberds, a research economist and senior policy adviser at the Federal Reserve Bank of Atlanta, personal data collection creates some consequences—or “externalities,” in the parlance of economics—in the normal course of enabling consumer payments. An externality is an unintended side effect of a transaction imposed on those who are not party to the transaction. A positive externality, for example, is when your neighbors plant a rose garden for their own benefit, but you also benefit because you enjoy the beauty and fragrance of the flowers whenever you walk by their yard.

On the other side of the spectrum, Roberds says, is the negative externality that banks and other payments providers create whenever they verify payer identities by collecting personal data. “As more and more of that data is assembled and it becomes more and more extensive,” says Roberds, “it becomes a [broad] target for theft by talented individuals who are able to access that data, use that [data] to construct pseudo-identities that allow them to illegitimately purchase goods and services, and thereby impose costs on everyone else who’s working within the credit system.” Because the banks and payments providers do not bear the full cost of this criminal activity—they cannot reimburse victims for time spent dealing with identity theft, for example, nor for damaged reputations—they collect more personal data than they really have to. This over-collection of data continues in part because there are so many different entities active in the payments system, making coordination difficult among the diverse parties.

Security as a weakest-link public good

At the same time that private companies are over-collecting personal data, they may be under-providing beneficial public goods. Public goods are products and services that can be consumed by more people at no additional cost. The late economist Jack Hirshleifer, who taught at the University of California, Los Angeles, discussed a specific subset of public goods as the weakest-link public good. A classic example of this kind of public good,



in Hirshleifer’s mind, is a dike system that provides flood protection to a below-seawater area. The dikes provide protection—but only so much as the shortest dike in the system. Said Hirshleifer, “If the dike is not breached, little to no loss will be suffered, but once breached, even by a little bit, the whole structure may give way.”

In the payments world, the level of protection that consumers get is determined by whoever makes the least effort to maintain his or her portion of the system. In other words, the security of payments data often functions as a weakest-link public good. According to Roberds, “Data is only as secure as the weakest place within the system that’s using it in terms of its security and its ability to be breached by hackers and other malefactors who would like to exploit the credit system.” Consequently, the security of the total payments system depends on the actions of those players who have the least to lose in the event of a data breach—or those who are the least savvy in implementing security standards.

Google’s chief economist, Hal Varian, explored what economists call the unequal incentives dilemma of weakest-link public goods in a 2004 paper, “System Reliability and Free Riding.” He concluded that the participant with the lowest benefit-cost ratio would determine the amount—of security, in this case—provided. In terms of data breaches, those companies with low revenues but high security costs will determine the level of protection for the entire industry. Furthermore, the U.S. payments industry includes many small merchants accepting card payments as well as technology start-ups offering new electronic payment products on a shoestring budget, which may make consumers more vulnerable to breaches. Start-up companies often have less risk-management experience and less to lose than more established firms, but a breach of one of these small players may pose broader threats to the integrity of the payments system.

A self-policed marketplace

Economic theories about externalities and weakest-link public goods illustrate how excessive data collection and poor risk mitigation can result from mismatched incentives. Payment systems are a type of shared infrastructure facilitating economic activity, very much like the highway system or postal service.

In the payments world, the level of protection that consumers get is determined by whoever makes the least effort to maintain his or her portion of the system.



This view of the payments system as a shared infrastructure explains why in many countries the government plays a strong role in managing payments.

In the United States, though, it's the market that provides and manages payments. This country's free-market approach has created a robust and innovative payments industry—but it has also created problems. Specifically, negative externalities and under-provision of weakest-link public goods may be major contributors to the increasing incidence of data breaches in the United States.

To date, the payments industry has managed many of the risks through market mechanisms. Pricing is one such tool. For example, part of the reason that credit cards cost more than debit cards for merchants to accept is that credit cards have a higher incidence of fraud. Insurance, another tool, ensures that most participants protect themselves against risk. Card issuer guarantees, whereby the issuers promise to pay merchants when the merchants accept their cards, are yet another tool. Making such guarantees motivates issuers to keep the credit risk of their cardholders low.

The industry also manages risk through self-regulation. Card network rules, for example, require that merchants follow certain standards or risk losing the right to accept cards. Private contracts between merchants and their banks may require that participants meet card network security standards like the Payment Card Industry Data Security Standard (PCI-DSS). Contracts may also require that parties make specified anti-fraud efforts or face increased liability for losses.

Unfortunately, criminals are also increasingly sophisticated. As data security threats evolve, the market's ability to manage risk may be challenged. For example, Cindy Merritt,

assistant director of the Atlanta Fed's Retail Payments Risk Forum, recently commented on the value of PCI-DSS in the United States today in the Atlanta Fed's blog dedicated to payments security issues. She said that although PCI-DSS is the current industry security standard for merchant card acceptance, "[a]s schemes become increasingly sophisticated, however, these guidelines will likely be less and less effective—a possibility that should give the industry pause."

Merritt's concerns highlight the fact that sometimes the market may not be able to adequately align incentives or ensure cooperation in fighting data breaches and financial crimes. In such cases, there may be a role for regulatory intervention. Well-designed regulations can support industry efforts to coordinate risk management and enforce standards.

Despite the generally robust market response to risks in the payments industry, government intervention is appropriate when market failures result in data breaches. Regulators have the ability to offer incentives for private companies to provide more public goods, like payments data security, and disincentives for creating negative externalities, like the over-collection of data. Regulators and industry working collaboratively can prevent data breaches. That way, you won't have any unpleasant surprises when you open your credit card statement. ■

This article was written by Jennifer C. Windh, a payments risk analyst in the Retail Payments Risk Forum at the Atlanta Fed.

