

Identity Theft: A Fast Growing Problem

Identity theft is one of the fastest growing criminal activities. A recent study by the Federal Trade Commission concluded that almost 3.25 million Americans have been victims of some type of misuse of personal information.¹ Retailers—especially successful retailers—are prime targets of identity thieves. Credit card transactions, private label credit cards, and customer loyalty and rewards programs all create a treasure-trove of information that can be immediately turned into dollars on the black market. The FBI estimates that U.S. businesses lose \$67.2 billion per year to computer crime, according to a recent article in *USA Today*.² The article describes organized online criminal forums where identities are bought and sold, with typical prices ranging from \$500 for a credit card number with personal identification number (PIN) code down to as little as \$7 for a credit card number with just the expiration date.

Virtually every advance in human history has a dark side—the law of unintended consequences. For retailers, part of that dark side is identity theft. Information technology (IT) has paved the way for retailers to handle consumer information and credit far faster than in decades past and to expand their operations to a truly global audience. But the ease and advantages of IT bring with them exposure to the unscrupulous among us who happily exploit any “holes” in a retailer’s information-handling processes, stealing the identities of customers and using that information to disguise shady activity and rack up huge debts.

The chain of events—from an external hack to an inside job to dumpster diving—and the responsibility for the losses that follow inevitably make their way back to the retailer whose system was breached. And beyond the financial loss, the retailer incurs costs to comply with a patchwork of privacy regulations as well as suffering damage to its reputation and livelihood. Many customers fearful of suffering identity theft then opt to shop elsewhere.

Why Traditional Insurance Policies Won't Protect You

Many insurers use forms developed by Insurance Services Office, Inc. (ISO). Others often use the ISO forms as a starting point, adding or deleting coverage to tailor policies to their own needs and the needs of their clients. Two of the primary forms used to provide coverage are the Building and Personal Property Coverage Form and the Commercial General Liability Coverage Form. Originally drafted in the early 1980s, these forms have undergone a number of revisions over the years in response to various events, including court interpretations of the coverage provided and changing exposures to risk.

Three decades ago, when the original forms were drafted, the Internet was only getting started as a commercial and interpersonal means of communication. The concepts of cyberspace, cybersecurity, cybercrime, cyberinsurance—cyberanything—were virtually unknown. These standard policies did not address such issues as identity theft.

In recent years, there have been various claims involving data and the Internet that ended up in various courts. Rulings conflicted with one another, largely because they addressed issues not anticipated in the ISO forms. ISO has since revised these and other forms that specifically address the scope of coverage available—and not available—for claims involving the Internet, data, and other like issues.

Most primary property and commercial general liability insurers now impose mandatory data corruption and cyberrisk exclusions. As a result, the coverage in traditional policies for data-related events, such as identity theft, is spotty at best. Thus, retailers are better served by purchasing policies specifically intended to cover the risks associated with their increasing reliance on technology and the perils of handling private and confidential information.

1. “Identity Theft,” U.S. Department of Justice, http://www.usdoj.gov/usao/mt/identity_theft/.

2. “Cybercrime flourishes in online hacker forums,” *USA Today* (posted October 11, 2006).

Identity Theft: A Fast Growing Problem

January 2007

All Retailers at Risk

At one time, it may have appeared that the primary targets of identity theft would be online enterprises and their customers. But it has become increasingly clear that “click-and-brick” enterprises are just as vulnerable and possibly more clearly in the cross hairs of the criminal community that has sprung up to acquire and exploit stolen personally identifiable information. Virtually all retailers store customer data whether or not they have an online presence, and there have been many attacks in recent years on such establishments—from both without and within. Some of what’s at risk includes:

- unwanted regulatory scrutiny and exposure to penalties for violation of the growing number of privacy regulations;
- business interruption and extra expense, both online and in-store, while compromised IT systems are repaired; and
- class actions brought by customers whose identities have been stolen involving not only fraudulent financial activity attributed to them, but also their costs to reclaim their status as it was before the breach.

Fortunately, the insurance industry has developed a suite of policies that can protect retailers against many of these risks, both the first-party damages and the third-party liabilities.

In addition to such risk-transfer solutions, retailers should also assess their IT systems enterprise-wide. While it is important to have insurance in place as a fail-safe measure, it is just as important—and far less costly—not to have the loss occur at all. Thus, retailers need to find and mitigate vulnerabilities in an effort to avoid breach of their IT systems.

Marsh has been at the forefront in designing and refining many of these solutions for nearly a decade. For more information on these specialized solutions, contact:

Robert Parisi
(212) 345-5924
Robert.Parisi@marsh.com

Repairing the Damage

There is no such thing as a 100 percent secure network. But as with the three little pigs, you can build your IT protection with straw, with wood, or with bricks. The stronger your protections, the more work potential identity thieves will have to do to break into your system. But even brick houses—and click-and-brick companies—can be breached.

If despite best efforts, the identities of a retailer’s customers are stolen—by hackers or by insiders—there are steps that can mitigate the damages. A proactive stance will likely be viewed more favorably by customers, regulators, and shareholders alike. The steps include:

- notifying customers of the breach as soon as practicable—but correctly by;
- providing customers with a solution in the same communication as notice of the breach.

Individual restoration can be daunting. The more a retailer does to help ease customers’ fears and burdens, the more likely those customers will remain customers—and the less likely the retailer will become involved in costly and time-consuming litigation.

Kroll, one of Marsh’s sister companies, offers a wide array of fraud services and solutions, delivered by seasoned professionals with years of experience, that can help retailers and their customers prepare for and recover from the aftermath of identity theft. For more information, contact:

■ Gina Sapp
(615) 320-9800, extension 1036
gsapp@kroll.com

The information contained in this publication is based on sources we believe reliable, but we do not guarantee its accuracy. This information provides only a general overview of subjects covered; is not intended to be taken as advice regarding any individual situation or as legal, tax, or accounting advice; and should not be relied upon as such. Recipients of this publication should consult their own insurance, legal, and other advisors regarding specific coverage and other issues.

Marsh is part of the family of MMC companies, including Kroll, Guy Carpenter, Putnam Investments, Mercer Human Resource Consulting (including Mercer Health & Benefits, Mercer HR Services, Mercer Investment Consulting, and Mercer Global Investments), and Mercer specialty consulting businesses (including Mercer Management Consulting, Mercer Oliver Wyman, Mercer Delta Organizational Consulting, NERA Economic Consulting, and Lippincott Mercer).

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Marsh Inc., except that clients of any of the companies of MMC need not obtain such permission when using this report for their internal purposes, as long as this page is included with all such copies or reproductions.

Marsh. The world’s #1 risk specialist.®

Copyright © 2007 Marsh Inc. All rights reserved.