Navigating the perfect storm

A white paper exploring the causes, consequences and resolution of corporate data breach

Experian™
Navigating the perfect storm

The digital nature of today's marketplace has given rise to a storm of identity theft, fueled by the convergence of three previously independent trends.

When organizations expose personally identifiable information (PII) on a massive scale, this is referred to as a data breach. Thieves acquire the exposed data, and the ensuing identity theft sustains a black market economy based on stolen data and deceptive exploitation.

As a steward of consumer and business information, Experian holds a profound and abiding respect for maintaining the public trust. We have invested a tremendous amount of time and energy to help organizations prepare for, respond to and successfully mitigate the consequences of a data breach.

To that end, this paper examines:

- Three trends that enable fraud and identity theft
- Current data breach statistics
- The costs of poor data breach management
- Fraud and identity theft causes
- How affected individuals respond
- Successful data breach resolution strategies

**Trend No. 1: dominance of the Internet**

The Internet has emerged as the preferred interface for global communication. Tech-savvy criminals exploit this online environment by obtaining, transporting and manipulating sensitive information to enable identity theft.

Thieves use the Internet to acquire data because organizations use it to transfer immense quantities of information at breakneck speed, inviting recipients to expose their PII across multiple online locations. Hackers or malicious programmers can intercept and compromise that process—a practice more commonplace than most companies would care to admit.

Thieves also use the Internet to move data: Social Security numbers, physical addresses, passwords and account numbers are bought and sold on illegal, underground e-commerce sites. This activity perpetuates a covert market for lost and stolen data that can transform mercenary hackers into wealthy entrepreneurs.

Sophisticated programmers turned criminals aren't the only ones capable of profiting from rogue data. Even petty thieves—who may steal a laptop with the simple intention of selling the hardware—will quickly recognize the greater value of information stored within.

Finally, thieves use the Internet to manipulate data. They depend on Internet-based programming languages to automate the data entry for hundreds of thousands of loan applications in seconds. The Internet also provides tools for modifying credit files. By changing billing addresses, identity thieves can divert new credit cards (and collection notices) away from their unsuspecting victims.
Navigating the perfect storm

**Trend No. 2: unprecedented credit dependency**

As credit use among consumers continues to eclipse the traditional notion of cash as a viable payment option, commerce is leaning more heavily than ever on alternative, non-cash forms of payment.

Prevailing market forces as well as legislation have persuaded Experian, Equifax and TransUnion, the three major credit reporting agencies, to expedite consumers’ ability to access and even update their own personal credit files. While this expanded control is a boon to the individual consumer, it’s an even bigger gift to sophisticated imposters and criminal fraudsters who potentially enjoy the exact same degree of access and control.

The instant accessibility of the Internet has also contributed to strong consumer demand for instant credit. Businesses have responded in kind, adopting newer, riskier channels in a race to meet the demand.

**Trend No. 3: inexpensive data storage devices**

The availability of portable data storage devices has permitted identity theft to reach astounding economies of scale. Consider that in 1960, a truck would be required to steal a million hard files; today an identity thief can steal just as many with a PDA. This trend has organizations scrambling to control and protect access to sensitive information.

Over the past 50 years, data storage device capacity has advanced dramatically while price and size continue to decrease. The 1960s saw the advent of magnetic tapes, followed by cassettes. These gave way to compact discs and personal computers, which led to cell phones, laptops and PDAs. High-density DVDs are part of the next wave in developing gargantuan storage capacities in small, portable data storage devices.

**A storm is brewing on the horizon**

Alone, each of these trends expands the arsenal of tactics used by criminals to steal information. Combined, they create a perfect storm of opportunity for rampant fraud and identity theft. A storm of this magnitude is most vicious when an organization data breach occurs. Thieves are able to maximize the payoff through millions of stolen records in a single event.

Subsequent events can ruin even the most fiscally sound organization: an employee loses a laptop containing a quantity of sensitive records. A thief finds the device, examines the contents and sells the stolen data. Using the stolen data they purchased, international criminals devise systems that automate new account fraud on a massive scale. Due to a lack of experience, the employee’s organization responds poorly and then suffers an onslaught of legal, financial and brand-related damages.

Ten years ago this scenario was impossible. Today, it’s frighteningly routine.

**2005 — the first “perfect storm”**

As chronicled by the Privacy Rights Clearinghouse, the confluence of the three trends just described was first felt Jan. 10, 2005, when information technology engineers at George Mason University discovered that the names, photos and Social Security numbers of 32,000 students and staff had been compromised by an attack on the university’s primary identity server. It was an event both embarrassing and foreboding: the first recorded incident of a large-scale data breach. The first perfect storm of massive information loss had arrived.

Since 2005 when the Privacy Rights Clearinghouse began tracking data breach incidents, more than 250 million customer records containing sensitive and confidential information have been lost or stolen. An examination of year-over-year increases in data-breached consumer figures reveals these patterns:

- The annual frequency of reported data breaches is rising rapidly
- The total number of breached records is growing exponentially
- The total cost of a data breach continues to increase every year, resulting in serious financial consequences for an organization

---

1 See the Privacy Rights Clearinghouse Web site, www.privacyrights.org, for more details about this ongoing data breach tracking survey.
Navigating the perfect storm

The escalating costs of poor data breach management

Most companies calculate their customer acquisition and retention costs. The cost of a data breach is determined by the impact on an organization’s customer base multiplied by the cost of replacing those customers.

The respected independent research firm Ponemon Institute publishes an annual report detailing the financial impact of data breaches on organizations nationwide.

According to this year’s Ponemon Institute “Fourth Annual US Cost of Data Breach Study” (January 2009), the average cost of a data breach has risen to $202 per individual record from $197 in 2007. The report clearly illustrates the potentially disastrous financial outcome that can befall organizations that fail to appropriately handle compromised information in a timely manner.

Breaches affect employees and customers

In an American Payroll Association survey, 85 percent of employees believe their employers adequately protect their vital personal information. In the same survey, 41 percent of technical professionals believe their respective companies are not effectively enforcing data protection policies.

The chasm between these two perspectives is telling. Employees want to believe their data is safe, but when a breach occurs and the assumption of safety is suddenly dismantled, staff reaction can be severe.

Companies that delay or mishandle breach notifications are also four times as likely to experience customer turnover as companies that handle them quickly and clearly.

Faced with those numbers, companies should do everything they can to minimize flight and maximize customer loyalty with proactive protection against fraud and identity theft. Given the opportunity, 70 percent of consumers would take action to prevent being a victim if they only knew what to do.

Credit monitoring is a low-cost alternative to the financial consequences a breached business may incur. Experian’s Triple AdvantageSM and Triple AlertSM credit monitoring tools have helped reduce the potential fiscal damage of a data breach for over 1,000 organizations by mitigating the most expensive aspect of the event: lost business.

The causes and consequences of identity theft

The most common causes of compromised information at the corporate level are human negligence and theft. Lost or stolen desktop computers, laptops, PDAs or flash drives constitute 49 percent of data breach cases. In fact, more than 80 percent of firms responding in the 2006 Ponemon Institute study had put critical data at risk by losing a laptop containing sensitive information.

Identity thieves waste no time setting up new accounts and billing addresses. Since the new victims never see a bill, they have no idea other accounts are now open in their names. On average, the identity theft victim doesn’t discover the problem for 13 months, costing an estimated $1,173 and 175 frustrating hours to repair the damaged credit record.

3 USA TODAY, 11/13/2006
4 Ponemon Institute, 2006
5 “National Survey Data Breach Notification,” PGP, 2005
6 “National Survey Data Breach Notification,” PGP, 2006
Navigating the perfect storm

The data breach solution — swift, comprehensive crisis management

It’s no accident that organizations with the best track records for handling data breaches are industry leaders in their respective fields. Hundreds of these businesses have endured severe information compromise and emerged on the other side with relatively minimal cost, no litigation and stronger customer loyalty.

How? By understanding and responding according to the perspective of the victims. Employees, customers and consumers do not blame companies for lost laptops — they blame companies for pursuing corporate concerns ahead of their own. In all cases, one factor has determined success or failure: swift, comprehensive crisis management.

By demonstrating sound financial and ethical leadership in the midst of a high-risk situation, executives can mitigate the consequences of a data breach, preserving customer loyalty and guarding brand equity.

Professional data breach resolution

Leverage the expertise of Experian to give your business every opportunity to successfully manage the data breach storm. As the nation’s leading credit monitor, Experian has developed dozens of successful partnerships with Fortune 100 companies and government agencies across all industries. We work with chief privacy and security officers, legal counsel, information technology engineers and human resource directors to resolve each unique situation.

Experian manages the entire resolution process to minimize cost, mitigate risk and maximize customer retention. Our experience with high-profile cases is unmatched. Our team has responded to the largest, most severe and public breach cases in U.S. history. This expertise — including our reliable data assets, advanced technology and specialized response team — offers you peace of mind in the midst of a crisis.

Additionally, Experian’s Triple Advantage and Triple Alert credit monitoring services offer post-breach notification strategies, fraud resolution assistance, tri-bureau credit reports, suspicious activity alerts, and outstanding support against the threat of identity theft for employees and customers.

Resolution plan development

In the days following a data breach, Experian works with each unique client to identify the legal, financial and business issues that must be addressed. This analysis includes a determination of the organization’s ability to respond to the incident, the body of information at risk and the various types of audiences affected. The objective is to move as quickly and safely as possible toward a state of complete operational readiness. Once the response plan is prepared, notification begins.

Customer notification compliance

State- and industry-specific data breach legislation favors the individual. The majority of states require immediate, public data breach disclosure. Even if companies are not headquartered in states with legislative requirements, they may be subject to disclosure laws if they have customers in those states. Certain industries are required to disclose information regardless of location.

To help organizations meet state, industry and legal requirements, Experian offers a suite of data breach resolution services that include notification letter drafting, printing, shipping and e-mail services.

Fraud resolution assistance

Victims of identity theft incur real costs and thus have legal recourse against the responsible parties. An organization’s best defenses against this action are a comprehensive fraud resolution product coupled with reimbursement for expenses related to losses caused by any resulting identity theft. In recognition of this concern, Experian offers meticulous, comprehensive fraud resolution assistance, assigning an experienced fraud resolution representative (FRR) to each victim.

Data fraud cases require many agencies and services working in concert. An identity theft victim acting alone in the hope of effectively managing his or her own case would quickly become overwhelmed by the sheer complexity of the task. The FRR coordinates multiple-agency efforts, drawing on years of fraud expertise to act as a dedicated resource until the case is completely resolved.

Fraud resolution support begins when a customer contacts us to report suspected fraudulent credit activity, followed by a detailed report and clear plan of action.
A fraud resolution representative offers:

• **Credit and account resolution.** The FRR investigates the incident and contacts the pertinent credit grantors to close accounts, compile documentation and escalate the case beyond local authorities if direct action is not taken.

• **Government and law enforcement assistance.** The FRR also helps victims contact all relevant government agencies and law enforcement officials, including the Department of Motor Vehicles, the Internet Crime Complaint Center, the U.S. Postal Inspection Service and the Federal Trade Commission.

**Tri-bureau credit monitoring**
Credit monitoring is the best safeguard against the misuse and exploitation of stolen or lost personal information. Identity thieves can access, manipulate and leverage nearly every safeguard used by companies to identify genuine clients, including Social Security numbers, addresses, maiden names and birth dates. While most financial institutions offer account monitoring and notification for existing accounts, if an identity thief orders a new credit card from a new bank using a new billing address, the victim will never be notified.

In light of this accessibility, single agency credit monitoring is an incomplete, insufficient fix. Anything less than a tri-bureau solution leaves the client blind and vulnerable to warnings that demand immediate, aggressive action. Experian facilitates the detection of potential fraud by flagging suspect credit report activity on all three national credit reporting agencies and alerting the consumer — all within 24 hours of the event in question.

Depending on the scope of the data breach, Experian offers several tiers of monitoring and alerts. Registration via the Internet, phone and mail expedite the establishment of these services.

**Real-time alerts and expert support**
Once registered for credit monitoring, consumers affected by a data breach are notified of any key changes in report activity. This includes new accounts, inquiries, address changes, delinquencies and public records. Various features allow consumers to track scores online over time; view credit reports; and access proprietary content on fraud resolution, credit monitoring and identity theft.

Since Experian has managed more data breaches than anyone else, our specialists have resolved nearly every question, every inquiry — every imaginable scenario. If, at any point in the resolution process, consumers have difficulties or questions, a fraud resolution representative is ready and willing to help.

**Successfully navigate every storm**
As a global information steward, Experian has conducted research identifying the three trends explored in this article, which continue to fuel the rising frequency and severity of corporate data breach incidents:

• **Pervasive Internet usage by businesses and consumers**
• **Unprecedented consumer credit dependency**
• **Higher-volume data storage capacity in ever-smaller devices**

Together, these trends have converged to create an atmosphere that promotes the theft of massive quantities of information. Regardless of the causes, research shows a data breach must be managed with discretion, speed and integrity. Organizations that mismanage the crisis or delay notifying affected individuals can expect staggering breach resolution expenses. Of that amount, a significant portion is due to lost business, a figure that can be significantly reduced through expert breach resolution assistance.

Experian has developed Triple Advantage and Triple Alert credit monitoring services in response to these potential business losses. Used by over 1,000 organizations and more than 20 million consumers, these world-class tools help you rapidly and properly mitigate the risks that can arise from a data breach.

For more information, please call Experian at **1 866 751 1323**.