

---

---

THE CENTER

FOR INFORMATION  
POLICY LEADERSHIP

HUNTON & WILLIAMS LLP

---

---

## **INFORMATION SECURITY BREACHES AND THE THREAT TO CONSUMERS**

by  
Fred H. Cate  
September 2005

The Center for Information Policy Leadership develops initiatives that encourage responsible information governance in today's digital society. The Center is a member-driven organization that operates within the Privacy and Information Management practice at Hunton & Williams LLP. Through collaboration with industry leaders, consumer organizations and government representatives, the Center provides leadership in developing policy to help ensure privacy and information security while balancing economic and societal needs and interests in today's global information age. [www.informationpolicy-center.com](http://www.informationpolicy-center.com).

## Summary

- Information security “breaches” take many forms and occur in a wide variety of settings. However, contrary to recent press reports, they do not appear to be increasing.
- Research indicates that only a small percentage of breaches result in any harmful use of data.
- Account fraud and true identity fraud — the two identity-based frauds most feared by consumers and policy makers — are actually declining.
- The vulnerability of unsecured personal data and the threat of identity-based frauds nevertheless continue to grow and evolve as perpetrators become more sophisticated in how they seek to obtain and exploit personal information.
- That threat, and particularly the risk of synthetic identity fraud, poses real dangers for individuals, institutions, and the information economy.
- Action to combat that threat must be thoughtful, well targeted, and forward-looking if it is to guard against new risks and do so without compromising the information-based services that the public increasingly enjoys and expects.

## Introduction

The unprecedented number of disclosures about information security “breaches” during the first half of 2005 has brought into sharp focus the importance of securing personal information. To date, however, concerns about vulnerabilities in information systems have not consistently translated into a better understanding of threats to information, the tools available for securing it, or the challenges faced in employing those tools. In short, the perceived need to “do something” threatens to overwhelm the need to first understand what needs to be done.

This paper highlights what we know about recent breaches, the risks they pose for individuals and institutions, and the important lessons we have learned about information security threats, tools, and priorities. Future papers will address other aspects of information security and the tools available for protecting it.

The lessons from recent breaches and related information security research demonstrate that the risk to consumers of most breaches is not as great as popular rhetoric suggests. However, unchecked, information security breaches pose real risks for individuals, institutions, and the information economy. Moreover, the threat is constantly evolving to exploit weaknesses in data protection. Understanding those risks and their changing nature is critical to ensuring that new laws, technologies, and other measures target the most serious threats and provide the public with real security.

## Recent Breaches

- **There is no evidence that information security breaches are increasing.** The numerous disclosures about breaches during the first half of 2005 resulted from a combination of a significant

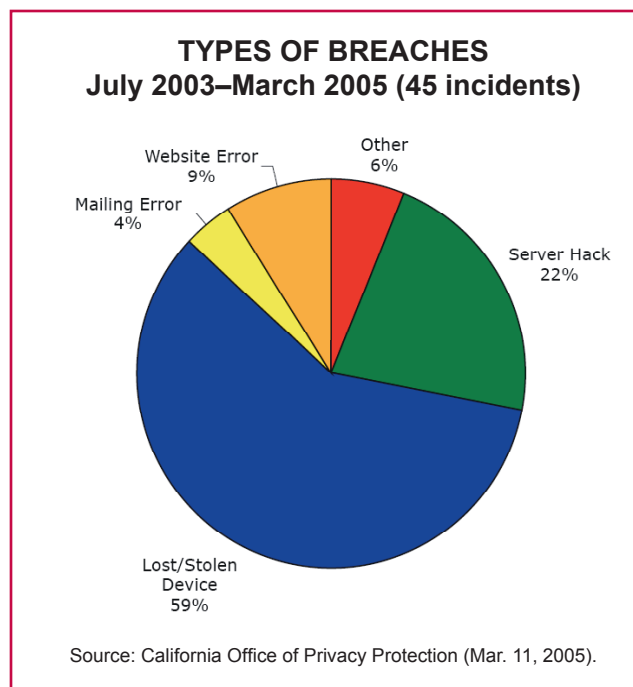
## Examples of Types of Security Breaches (2005)

Type of Breach	Recent Examples and Dates Announced
Fraudulent account created	ChoicePoint (2/15/05)
Stolen laptop/computer	UC Berkeley (3/11/05); NV Dept. of Motor Vehicles (3/12/05); MCI (4/5/05); CA Dept. of Health Services (4/15/05); Motorola (5/30/05); Bank of America (7/29/05)
Hacking	DSW/Retail Ventures (3/8/05); Boston College (3/11/05); Northwestern Univ. (3/20/05); Polo Ralph Lauren/HSBC (4/14/05); CardSystems (6/16/05)
Passwords compromised	LexisNexis/Seisint (3/10/05)
Theft by insider/employee	GA Dept. of Motor Vehicles (4/05); Wachovia, Bank of America, PNC Financial Services Group, & Commerce Bancorp (4/28/05); Univ. of Hawaii (6/18/05)
Missing back-up tape	Bank of America (2/25/05); Ameritrade (4/20/05); Time Warner (5/2/05); CitiFinancial (6/6/05); City National Bank (7/6/05)

Source: Privacy Rights Clearinghouse ([www.privacyrights.org/ar/ChronDataBreaches.htm](http://www.privacyrights.org/ar/ChronDataBreaches.htm))

number of breaches involving data about many consumers and a California law requiring entities that maintain personal data to disclose when those data may have been acquired by unauthorized users.<sup>1</sup> Under the California law, it does not matter whether the breach was deliberate or accidental or whether the data were misused. Most businesses have chosen to provide the notices required under the law to all U.S. residents affected, not just those in California.

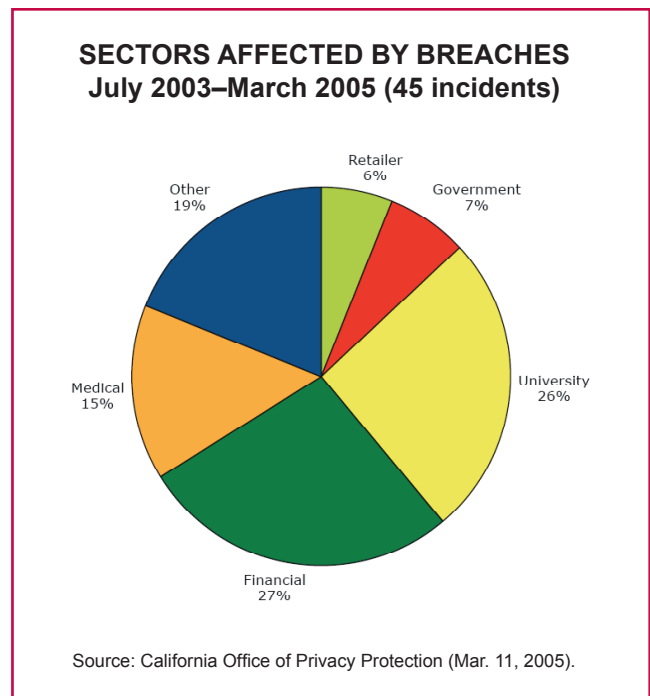
- **Information security “breaches” take many forms.** These include lost or misplaced disks or backup tapes, stolen laptops and cell phones, hacked data, improperly secured websites, data lost or stolen in transit, information taken by rogue employees, misdirected mail, and many other forms. California data suggest that most are accidents, rather than the result of deliberate attacks, and many are not so much “breaches” as incidents in which data may — or may not — have been compromised. Most of these incidents do not involve the Internet or other digital technologies. In fact, many involve lost or misplaced information or equipment, rather than theft.
- **Breaches occur in a wide variety of settings,** including many industry sectors, government agencies, universities, and the not-for-profit community.



→ **It appears that only a small percentage of breaches actually involve any harmful use of data.** There are many reasons for this, including:

- Many incidents described as information security breaches involve no effort to misuse data at all. Data may be lost, rather than stolen, or obtained incidental to the theft of some other valuable commodity and discarded or destroyed without ever being accessed (for example, a laptop that is stolen for the value of the machine and immediately wiped clean so that it can be used by someone else).
- Not all attempted misuses are successful; industry efforts to detect and block fraudulent charges and illicit access to accounts are highly successful. The financial services industry, for example, intercepts and blocks many fraudulent credit card charges.
- Even the portion of those efforts to misuse personal information that are successful usually result in no financial or physical harm to consumers. The most recent data available indicates that 67% of victims of identity-based frauds report suffering no economic loss and paying no out-of-pocket expenses. The costs were usually paid by businesses, and ultimately by all consumers.<sup>2</sup>

As a result, many of the breaches that were reported as involving data concerning the largest number of people may in fact affect very few. Visa estimates that 2% of compromised credit card numbers are used fraudulently.<sup>3</sup> Other evidence collected in a July 2005 study by Thomas Lenard and Paul Rubin suggests that the percentage may be lower.<sup>4</sup>



→ **Information security breaches are among the least common ways that personal information falls into the wrong hands.** In 2005, for the half of victims of identity-based frauds who reported knowing from where their information had been obtained, the most common source of personal information, by a factor of two to one over any other category, was “lost or stolen wallet, checkbook or credit card.”<sup>5</sup> Family members and relatives along with friends and neighbors make up half of all known identity thieves.<sup>6</sup> Consumers often end up unwittingly providing thieves with access to sensitive data by failing to secure their own data, by responding to fraud schemes, such as phishing and pharming, and by careless use of their personal information.

## Identity-Based Fraud

→ **The risk most associated with information security breaches in the minds of many consumers and policy makers is identity theft or, more accurately, “identity-based fraud.”** That term includes a variety of crimes. Regulators and researchers usually divide these into three categories.

- The first and most prevalent is “account fraud.” Account fraud involves conducting unauthorized transactions on somebody else’s account (e.g., one person using another person’s stolen credit card). While this type of activity is facilitated by access to personal information (e.g., a bank account number or credit card number), it has little in common with the other forms of identity-based fraud and has existed as long as there were credit cards or checks to steal. Account fraud is usually easy to detect because the fraudulent transactions appear on the victim’s monthly account statements. Congress and state legislatures have adopted strict laws in an attempt to prevent and punish account fraud and industry is successful in blocking most efforts to commit account fraud.<sup>7</sup>
- “True identity fraud” involves opening a new account using the identity of another consumer. The victim may never know of the new account’s existence until he or she applies for a mortgage or loan and discovers the unknown account when the credit report is checked, or when the creditor attempts to collect on the debt from the victim after the perpetrator has defaulted. Congress requires the three national credit bureaus to provide consumers, upon request, with a free credit report each year to assist consumers in detecting true identity fraud early, before they need credit themselves.<sup>8</sup>
- The third and newest type of identity-based fraud is “synthetic identity fraud.” This involves combining the identity elements of real people with fabricated identity elements to create a new identity. Synthetic identity fraud poses significant risks for businesses and others that grant credit or provide products and services to the nonexistent, “synthetic” person. It also can harm the individuals whose information was combined and who later may be associated erroneously with the fraud. And it can be very dangerous for society more broadly if the frauds perpetrated by the creators of the synthetic identities become widespread or if those identities are used by terrorists to gain access to airplanes, government buildings, or other critical infrastructure. Synthetic identity fraud is the hardest to detect and may, in fact, not be visible for years, as thieves develop credit records for the new identities they have created.

Account fraud, true identity fraud, and synthetic identity fraud are three different types of crimes. While press reports and policy makers often lump them together, it is useful to treat them separately because they often involve different types of criminal activity and require different types of responses.

- **Account fraud and true identity fraud are not as prevalent as press reports suggest and do not appear to be increasing.** Two identical studies by Synovate that took place in late 2003 and early 2005 provide considerable insight into the reality of identity-based frauds. They show that the number of victims is declining in real terms and as a percentage of the U.S. population.

According to the 2005 Javelin study, 1 out of 23 adult Americans was a victim of an identity-based fraud in 2004.<sup>9</sup> That is a significant number, but it is a far cry from the claim in recent press reports that the figure is 1 out of 4. That claim appears to reflect more about the vagueness and breadth of the term “identity theft” than about the reality of how frequently these crimes occur. According to the FTC’s 2003 study, 38 percent of people who identified themselves as victims of “identity theft” said that they previously had reported the theft to no one — not even their own bank or credit card company — suggesting that even the 1 in 23 figure may be exaggerated.

Other evidence appears to confirm the findings of the Synovate studies. The 2005 Nilson Report on credit card fraud reports that the total cost of such fraud — according to the Federal Trade

	Synovate Studies	
	2003 (FTC)	2005 (Javelin)
Annual cost	\$51.4 billion	\$52.6 billion
Number of victims	10.1 million	9.3 million
% of U.S. adult population affected	4.7%	4.25%
Total resolution time	333.3 million hours	260.4 million hours
Median resolution time	33 hours	28 hours
% of victims who spent 9 hours or less on resolution	64%	68%
% of victims who paid no out-of-pocket expenses	63%	67%
% of thieves who are friends, family members, or neighbors	53%	50%
Sources: Synovate, <i>Federal Trade Commission — Identity Theft Survey Report</i> (2003); Javelin Strategy & Research, 2005 <i>Identity Fraud Survey Report</i> .		

Commission, the largest component of identity-based fraud — to card issuers decreased 10% from \$882 million in 2003 to \$788 million in 2004.<sup>10</sup> From 1992 to 2004, the Nilson Report found that the cost of credit card fraud had fallen by more than two-thirds from \$.157 to \$.047 per \$100 in credit card sales.<sup>11</sup> Fraudulent charges are lower as a percentage of credit card use in the United States than anywhere else in the world.<sup>12</sup>

## The Evolving Threat

- **Society’s growing reliance on information technologies exacerbates both the threat posed by personal information in the wrongs hands and the dangers of poorly focused or excessive regulation intended to guard against that threat.** Information today increasingly substitutes for personal relationships and for currency. This is especially true in Internet-facilitated transactions which include, for example, a majority of stock trades, consumer banking interactions, and airline reservations. Unfortunately, the convenience, customization, lower cost, and heightened consumer expectations that information enables also create new opportunities for abuse, as the development of identity-based crimes over the past decade demonstrates. As a result, the threat continues to grow and efforts to combat that threat inevitably run the risk of interfering with valuable information-based services.
- **There is ample evidence that both the risk of unsecured personal data and risks and the potential impact of identity-based frauds are growing and evolving.** For example:
  - Recent breaches demonstrate an evolution of attack strategies. As one vulnerability in information security systems was identified and patched, attacks evolved to target other weak spots. Moreover, as leading companies enhanced their information security, attacks have clearly increased against less well prepared institutions.

- Many identity-based frauds reflect key similarities — e.g., common addresses, phone numbers, targets, and strategies — that cause law enforcement officials to believe they are orchestrated by well organized and financed perpetrators. Information security breaches pose more significant risks as the sophistication of fraud rings increases.
- Historically, the large majority of reported identity-based fraud has involved either account fraud or true identity fraud. These are the types of fraud that most studies measure and that appear to be declining. There is emerging evidence, however, that synthetic identity fraud is growing. Synthetic identity fraud is harder to track and may take years to detect, but it appears increasingly clear that synthetic identity fraud accounts for a significant and growing portion of identity-related fraud.<sup>13</sup> Security breaches can significantly facilitate synthetic identity fraud by providing access to a large volume the disparate pieces of personal information about individuals often used to create synthetic identities.
- **Information security breaches pose real risks for individuals.** Compromised information can cause problems that are time-consuming and frustrating for individuals to remedy. The 2005 Javelin study reported that while two-thirds of victims lost no money and spent less than 9 hours remediating the results of identity-based frauds, the burden on the remaining third is so great that the average (mean) out-of-pocket cost per victim is \$650 and the time spent to resolve the fraud is 28 hours.<sup>14</sup> Moreover, breaches can threaten privacy and thereby affect consumers even if no identity-based fraud results.
- **Security breaches also pose significant risks for businesses.** One reason that the financial impact on consumers is relatively small is that most of the cost is borne by businesses. In 2004, U.S. business suffered \$50 billion in losses from identity-based frauds.<sup>15</sup> Moreover, businesses suffer even greater financial loss through the loss of consumer and market confidence when a breach occurs. A 2003 study found that firms victimized by an information security compromise that involved theft of credit card information suffered a stock market loss of 9.3% on the day the incident was announced, increasing to 14.9% over three days.<sup>16</sup> Lenard and Rubin noted that this “cost is quite large — three to five times the amount found in similar studies for other classes of events.”<sup>17</sup> Businesses also risk lawsuits, the cost of increased government oversight, and the burden of regulatory investigations and compliance.
- **The online economy is especially at risk.** Repeated studies show that consumers will stay away from electronic services, such as online banking, if they do not feel that their personal information is secure. This could significantly increase their vulnerability to identity-based fraud because information is statistically more secure online than offline. Moreover, online services are often more convenient and efficient and less expensive than comparable offline transactions. Online commerce has contributed significantly to nationwide competition and the availability of new and innovative services, so consumers and businesses could be seriously harmed if it lags. Even if tangible harm from security breaches is comparatively small, as indicated by recent studies, intangible harms and other fears can greatly increase the cost of such incidents. Those costs can be considerable for enterprises that rely on personal information, consumers, and the online economy as a whole.

## Conclusion

The lessons from recent experience and research indicate that the risk to consumers of information breaches is not as great today as news coverage might suggest. Nevertheless, there is still reason for

concern. Information technology is changing the way we do everything. Information is the currency of our lives; it has enormous value. That is why concerted efforts are underway to steal and misuse it. The threat is continuously changing to exploit weaknesses in data protection. As a result, the risk to consumers, businesses, and the economy is growing. Action to combat that risk is essential. However, that action must be thoughtful, well targeted, and forward-looking if it is to cope successfully with new threats and do so without compromising the information-based services that our economy relies upon and the public increasingly enjoys and expects.

## References

<sup>1</sup> Cal. Civ. Code § 1798.29.

<sup>2</sup> Javelin Strategy & Research, *2005 Identity Fraud Survey Report* at 3-4.

<sup>3</sup> Robin Sidel & Mitchell Pacelle, "Credit Card Breach Tests Banking Industry's Defenses," *Wall Street Journal*, June 21, 2005, at C1.

<sup>4</sup> Thomas M. Lenard & Paul H. Rubin, "An Economic Analysis of Notification Requirements for Data Security Breaches," *Progress on Point*, 12.12, July 2005, at 8.

<sup>5</sup> Javelin Strategy & Research, *supra* at 7.

<sup>6</sup> *Id.* at 3.

<sup>7</sup> See, e.g., The Identity Theft and Assumption Deterrence Act of 1998, which makes it a crime to knowingly transfer or use any means of identification with the intent to commit or facilitate identity theft. 18 U.S.C. § 1028.

<sup>8</sup> Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159 § 211(a), 117 Stat. 1952, 1968-70 (amending 15 U.S.C. § 1681j(a) (2000)).

<sup>9</sup> *Id.* at 12.

<sup>10</sup> "Credit Card Fraud in the U.S.," *Nilson Report* (Mar. 2005).

<sup>11</sup> *Id.*

<sup>12</sup> *Id.*

<sup>13</sup> ID Analytics, Washington briefing, Aug. 3, 2005.

<sup>14</sup> Javelin Strategy & Research, *supra* at 3.

<sup>15</sup> Lenard & Rubin, *supra* at 2.

<sup>16</sup> Ashish Garg, Jeffrey Curtis & Hilary Halper, "Quantifying the Financial Impact of IT Security Breaches," *Information Management & Computer Security*, vol.11, no. 2, 74-83 (2003).

<sup>17</sup> Lenard & Rubin, *supra* at 5.

## About the Author

Fred H. Cate is a Distinguished Professor of Law, Adjunct Professor of Informatics, and director of the Center for Applied Cybersecurity Research at Indiana University. A senior policy advisor to the Center for Information Policy Leadership at Hunton & Williams, he is a member of Microsoft's Trustworthy Computing Academic Advisory Board and of the National Academy of Sciences Committee on Information for Terrorism Prevention. The author gratefully acknowledges the thoughtful comments of Marty Abrams, Carolyn Brehm, Peter Cullen, Tom Oscherwitz, Jay Soloway, Lisa Sotto, and Orson Swindle. The author alone is responsible for the views expressed herein.