



THE NATIONAL DATA BREACH ANALYSIS

EXECUTIVE OVERVIEW

On February 15, 2005, ChoicePoint announced it had incurred a sensitive, large-scale data breach. Over the next six months, a broad array of organizations from banks, cable service providers, data aggregators, credit card processors, retailers and others announced almost 100 other breaches affecting over 50 million consumers.

These data breaches have put a national spotlight on corporate data security practices. They have also sparked consumer fears about a surge in identity theft because the sensitive data compromised in these breaches—Social Security numbers (SSNs), account numbers, driver's license numbers, etc.—are used by criminals to perpetuate identity and transaction fraud. Growing public insecurity about the safety of personal data has prompted state and federal law makers as well as regulators to take action.

However, consumers, industry advocates and regulators have rarely discerned between the different types of data breaches. To be sure, any data breach or theft of consumer identity data should cause alarm. But in fact certain data like personal identifiers carries a far greater risk of financial loss than other types. Other types of data carry a lower risk of harm, including credit card account numbers.

Despite the considerable amount of attention given to data breaches, little is known about them. Until now, there was no research on whether data breaches lead to identity theft. Nor has there been much focus on how to mitigate the harm of breaches once they actually occur.

In this white paper, ID Analytics attempts to address this research gap by examining publicly available information about data breaches as well as actual data breach files from four separate incidents representing approximately

THE NATIONAL DATA BREACH ANALYSIS

500,000 breached consumer identities. The paper provides a first-hand glimpse of how real fraudsters are actually using breached data to commit fraud. The paper also discusses how patent-pending technology can help organizations detect data breaches sooner, determine the best next steps following a breach, and ultimately limit the harm caused by criminal abuse of breached consumer data.

ID Analytics was able to conduct this analysis because of its ID Network®, the nation's first and only collaborative, cross-industry identity network developed for the sole purpose of preventing identity theft and related fraud. The ID Network consists of three billion identity elements submitted by leaders in the financial services, wireless and retail industries. ID Network Members have agreed that identity theft prevention requires collaboration across organizations and industries and have entrusted ID Analytics to develop and maintain the technology required for this effort.

This analysis is the first of its kind and represents the only body of knowledge to date that explores the actual impact of data breaches with respect to resulting identity theft.

KEY FINDINGS

- Many organizations face some degree of breach risk. An analysis of publicly available data, shows that the majority of breached identities were in the financial services sector (57%), but the majority of occurrences occurred in the education sector (46%).
- Data breaches vary significantly depending on the type of data stolen and the intent behind the breach.
 - Data breaches involving identity-level information (e.g., SSN, address, phone number) are likely to be more harmful to consumers and industry than those involving replaceable account numbers.
 - Deliberate identity-level breaches pose the greatest potential for harm to businesses and consumers. Accidental data breaches are less likely to be harmful than those resulting from an intentional “hack” or hardware theft.
- Resources available to fraudsters, not the size of a breach, determine the amount of fraud that will result from a breach.
- Fraud rings that acquire data from data breaches use sophisticated techniques to avoid detection. These sophisticated techniques can be detected using the ID Network and advanced analytical technologies. The ID Network can test any data breach file for misuse that includes identity-level consumer data.

THE NATIONAL DATA BREACH ANALYSIS

- Account-level breaches do not appear to lead to subsequent fraudulent openings of new accounts for credit or services.
- In certain targeted data breaches, public notification of affected consumers may have a deterrent effect. In one large-scale identity-level breach, thieves slowed their use of the data after public notification.

STATISTICAL HIGHLIGHTS

ID Analytics studied the level of suspicious misuse of identity information across the approximately 500,000 identities in the breach files. Statistical highlights from the findings include:

- Sixty-eight percent of the publicly reported breaches during the study period were intentional breaches. Additionally, the vast majority of the identity-level breaches (38 out of 54) were intentional breaches.
- Excluding the Card Systems breach, 60% of breached identities involved in the publicly reported breaches were “lost data” and not stolen.
- The calculated fraudulent misuse rate for consumer victims of the analyzed identity-level breach with the highest rate of misuse was 0.098 percent – less than one in 1,000 identities.
- The account-level breaches did not appear to result in subsequent identity theft (defined as fraudulent opening of new accounts for credit or services).

FOR MORE INFORMATION ABOUT
ID ANALYTICS' NATIONAL BREACH ANALYSIS,
PLEASE EMAIL MARKETINGINFO@IDANALYTICS.COM