



## MONITORING THE ENEMY WITHIN: REFLECTIONS ON A NEW INTERNAL DATA THEFT STUDY

Who steals data, and what do they do with it? Cooper Bachman of ID Analytics scrutinizes research from a dozen data thefts resulting in 1,300 attempted instances of data misuse.

Cooper Bachman, ID Analytics, Product Analyst  
August 12, 2008

While external data breaches involving household brand names such as TJX tend to grab more headlines, insider data thefts are emerging as compliance and reputational risks for organizations. Recent studies suggest that over 60 percent of data breaches originate from an internal source or event. One reason for this is that in today's data-rich environment organizations continue to struggle with the 'human element' at the heart of data security. It can be extremely difficult to balance the protection of sensitive data with granting access to employees who need it to complete their daily job requirements. To that end, organizations have implemented several new security measures including employee education programs, data access monitoring, and strict policies regarding USB ports and portable devices. Although these are steps in a positive direction, little has been done to study and understand how the data is exploited once it leaves an organization.

In late 2007, ID Analytics performed Analysis of Internal Data Theft, a study of more than a dozen incidents of internal data theft involving over five million identities from consumer and employee files across the government, education, and commercial sectors. The purpose of the analysis was to identify cases of identity fraud resulting from internal data theft in order to understand the behavioral patterns associated with misuse of stolen identities. The study also analyzed the types of goods and services that were targeted by individuals who unlawfully obtained sensitive personal information from their organization.

The findings further illustrate the need to protect sensitive data from not only external factors, but internal employees as well. The research team found the following trends among the cases of internal data theft reviewed:

- Fraudulent activity resulting from internal data theft tends to occur in close proximity to the office location where the data was removed.
- Personal data stolen by an employee is misused more frequently than data obtained through an external breach.
- The study group revealed a disproportionate amount of attempts to fraudulently obtain wireless phones. While this phenomenon could extend beyond internal data theft, this trend was not apparent in our prior research focusing on the harm associated with data breaches.
- Employees or fraudsters abusing internally stolen data behave remarkably similar to traditional identity thieves who have access to breached data. The majority of breached identities were misused for a period less than two weeks and fraudsters primarily used the Internet to apply for goods and services.

Over a dozen incidents of internal data theft consisting of over five million consumer and employee identities were reviewed by ID Analytics fraud analysts. Of these, eight incidents ultimately led to identity fraud, with over 1,300 cases of attempted fraud targeting bank card, retail card, and wireless providers. These cases represent behavior that is indicative of organized misuse, which is a concentrated effort to abuse a group of stolen identities.

Identity fraud is different than account fraud. Identity fraud deals with stolen or fabricated identity elements (e.g., social Security number, name, and address). One way to detect identity fraud is to examine new account initiations across companies and industries. In cases of fraud, many new accounts of multiple types are opened across different institutions. Account fraud is the misuse of an existing account that is discovered examining transactions. Account fraud only affects a single institution and a single account. The harm is financial loss and it is easily reconciled by closing the account and issuing new cards.

It is important to note that this analysis is focused on the use of stolen identities being utilized to open new credit, retail, and wireless accounts. This study did not include takeover of existing accounts such as direct deposit account (DDA) or new openings of collateralized loans (e.g., mortgages and automotive finance).

Specifically, the study analyzed the change in identity relationships within each internally breached population looking for anomalous linkages. For example, if a group of consumers had no prior relationships with one another, and then suddenly began applying for credit cards and wireless phones at a single address, this would be viewed as a suspicious or anomalous relationship change. Then, each suspicious case was analyzed in depth and reviewed for possible misuse of identity data. The time periods analyzed ranged from 10 months to more than 30 months after the date of the internal data theft.

## **Methods of Misuse**

The study performed temporal and relational analysis on over 1,300 cases of misuse. From these, four common patterns were highlighted.

### **1. Misuse of Data Occurred Within 20 Miles of the Internal Data Source**

The data analysis found a geographic relationship between where the data was stolen and where it was used. In some cases, the misuse was occurring as little as two to five miles from the place where the data was removed. It is important to note, that the research did not include local lenders such as credit unions or community banks. The misuse identified was based on information from national credit card issuers, retail lenders and wireless organizations.

If the data has in fact been purchased by a national identity fraud ring, it is expected to see pockets of misuse in geographic areas much farther from the data source. However, all misuse occurred locally relative to where the data was removed and indicates the individuals who obtained the data were either abusing it themselves or providing it to other perpetrators in their local area.

Although there was no evidence of distributed data, it is known that a marketplace exists for identity information. In the Data Breach Harm Analysis published in 2007, a similar study analyzed stolen identities that were readily available on the Internet. As part of this research, scientists found that exposed identities on the Internet typically had a higher rate of misuse than the average consumer. As long as the value and accessibility of personal data remains high, the threat of breached data reaching the Internet and being digitally disseminated remains.

### **2. Misuse Rates are Higher Among Identities Involved in an Internal Data Breach**

The risk associated with targeted internal data theft is greater than accidental breaches because of the intent underlying the breach. If a laptop is stolen from an unlocked car or a tape containing sensitive information is missing, the intent to use the data for the purpose of identity fraud is low. An employee may have simply left his car unattended while a thief saw an opportunity to obtain and sell valuable hardware. On the other hand if a disgruntled employee prints out identity information on 100 consumers, the breach now represents a heightened level of risk. The employee's motive to unlawfully obtain and abuse sensitive personal data creates a riskier scenario than a lost laptop. Individuals who are part of a targeted internal data breach are far more likely to have their identities abused due to the intent of the perpetrator.

The second variable to consider when evaluating the risk exposed by an internal data breach is the number of compromised identities. Using similar examples, if an individual's information is one of five million identities contained on a lost laptop, she is far less likely to be a victim of identity fraud in comparison to one of the 100 individuals whose information had been printed out by the disgruntled employee. Even in the unlikely event the lost laptop was acquired by an identity thief, it would take a single fraudster approximately 250 years to abuse a group of five million identities. However, a motivated fraudster with a list of 100 identities can cycle through the list rather quickly. Due to the resource limitations of fraudsters, individuals have a higher relative risk in small breaches than in large ones.

In relation to the eight incidents of internal data theft where harm was found, the rate of misuse was between 3 percent and 36 percent of the breached population. The internal breach within the highest rate of misuse (36 percent) was a targeted effort by an employee to steal data from their organization. The data contained the name and SSN for each employee and was used to fraudulently apply for wireless phones and bank cards. For the incident resulting in only 3 percent of the breached population being harmed, an employee improperly handled data in a way that exposed only a small portion of the population to identity fraud.

For several of the incidents of internal data theft the ultimate size of the breached file was unknown. For example, if an employee with access to identity data siphoned out information and the company was unable to track data access, the 'breached population' is unknown. For these cases the entire population in the relevant database was analyzed for misuse. Even so, identities exposed to one of these internal breaches were up to twenty-four times more likely to have their identity abused than the average consumer.

### 3. Wireless Phones are Becoming More Popular Targets

In previous research, fraudsters have demonstrated a preference for bank cards over retail cards or wireless phones when fraudulently applying for goods and services after a data breach. While activity related to bank cards did not completely dissipate, this study revealed a new trend of fraudsters using internal data to apply for wireless phones. After analyzing over 1,300 cases of data misuse stemming from the eight instances of harm, 69 percent of the total applications targeted the wireless industry. In two of the incidents, the research found over 95 percent of the fraudulent applications were for mobile phones.

In another study released by Javelin Strategy and Research in early 2008, researchers further highlighted the shift towards mobile technology and reported fraudulent wireless account openings have increased from 19 percent to 32 percent of new account fraud since last year. A possible explanation for this is a combination of the growing popularity of higher tech handsets and the competitive nature of the wireless industry.

As demand for smart phones and mobile Internet access increase, wireless providers are offering discounts on hardware to attract customers into new annual contracts. Individuals who have acquired personal data from an organization are able to exploit mark-downs by applying for new accounts, receiving a free or discounted smart phone, and then reselling the hardware for a profit of several hundred dollars per handset. The disgruntled employee has no intention of ever paying the recurring monthly bill and the account eventually charges off.

### **Evidence suggests this trend may continue.**

### 4. Misuse Related to Internal and External Breaches Exhibit Similar Behavior

Identities involved in internal data theft demonstrated strikingly similar behavior to traditional data breach victims in two main categories: strong application activity in the online channel and the duration of misuse for each identity was typically less than two weeks.

Employees or recipients of internally breached data mimicked the same application patterns as serial identity thieves. Five out of the eight incidents of internal data theft had over 80 percent of their

application activity online. Although there were cases where phone and direct mail channels were used, the Internet continues to serve as a 'faceless' medium used by fraudsters to prevent detection.

Secondly, the period of misuse for each internally breached identity was approximately two weeks. This is consistent with prior research done by ID Analytics and demonstrates the sophistication of those with access to the data.

## **The Enemy in Action**

The following two cases illustrate the temporal and relational patterns described in the previous four findings. Each of these case studies was included in the overall analysis and was discovered using breach analysis technology.

### **Case Study #1**

An organization found an employee emailing sensitive information related to their customers to a personal email account. After completing an analysis on the breached identities, analysts learned there was organized misuse as a result of the internal data leak. The analysts discovered that the employee had submitted 196 applications using 66 different identities over a two-month period linking to one unlisted wireless phone number. Even though this activity continued for two months, 161 of the applications were submitted over a period of 11 days. In order to try and mask the fraudulent activity, five different addresses were used throughout the credit application scheme: three apartments and two single family homes.

In previous studies performed by ID Analytics, research showed identity thieves minimize the points of contact for a given group of stolen identities. This may help the fraudsters better control the flow of information to service providers and help them obtain the fraudulent credit cards and mobile phones. In this case, the employee used a pay-as-you-go wireless phone and terminated the service once the credit scheme was complete.

The employee focused on submitting credit card applications online, with 99 percent of the applications distributed across five different bank card issuers. The perpetrator engaged in application "flurrying" where a group of identities is used to apply for several applications over a very short period of time and then replaced by the next group of identities.

### **Case Study #2**

An entirely different direction was taken by the individuals perpetrating identity fraud in this next case. An employee gained access to a number of identities through improper data management within the organization. Several of the office locations had issued thumbdrives to subordinates and transferred sensitive employee and associate information between offices. Moreover, a large portion of the organization had access to sensitive identity information on a daily basis, with limited to no access controls established. Data contained on the thumbdrives were not encrypted. The perpetrators involved in this activity sent out 44 applications to one address using 31 identities over a one year span. In one case, the address used was linked to a single family home only 4.7 miles from the data source.

As opposed to applying for bank cards, the identity thieves focused primarily on targeting the wireless industry. Ninety-six percent of the applications were for wireless handsets, 68 percent of which targeted one specific carrier. This behavior suggests identity thieves may be beginning to target the wireless industry in greater volumes. Combined with the growing popularity of the handset and the ease of obtaining a phone (through contract renewals, in-store promotions, online discounts, etc), industry experts suggest this trend may continue.

## **Learning, Preparation & Taking Action**

After assessing identity data provided by breached organizations spanning industries and sectors, this internal data theft study succeeded in providing a better understanding of the behavior associated with stolen identities and the level of risk associated with internal data theft.

Together, these findings illustrate the unique challenges faced by companies operating in a data-rich environment. Business leaders desire an unparalleled customer experience while trying to maintain the appropriate balance between data access and personal privacy. Compounded with the need to protect sensitive personal data and the rising probability of an internal data leak, reactive approaches to a breach event are becoming less feasible.

Organizations should implement internal and external mechanisms to proactively address data security needs, including ongoing monitoring that detects early evidence of misuse within customer and employee data, without interfering with daily business processes. In addition, if organizations suspect that they may already be a victim of a data breach, they must take immediate action to gauge the magnitude of the breach event.

##

*Cooper Bachman is a product analyst at ID Analytics, a provider of on-demand identity intelligence solutions based in San Diego, CA.*