Murdo, Patricia

From: newsnow@magserv.cuna.org on behalf of pyfer@mcun.org
Sent: Tuesday, January 10, 2006 6:05 PM
To: Murdo, Patricia
Subject: CUNA News Now - ID theft risk not as great as expected, says study

ID theft risk not as great as expected, says study

SAN DIEGO, Calif. (1/11/06)--An analysis of four data breaches involving about half a million consumer identities reveals that few of the breached identities were misused for criminal financial gain, says a California-based identity risk management company.

Credit union members were among those whose personal information was compromised in several high-profile data breaches last year.

Different breaches pose different degrees of risk, found ID Analytics Inc., which conducted the study. The San Diego-based firm's research distinguishes between "identity-level" breaches, where names and Social Security numbers are stolen, and "account-level" breaches, where only account numbers, sometimes associated with names, are stolen.

The degree of risk varies based on the nature of the breach--for example, whether the breach is the result of a deliberate hacking into a database or a seemingly unintentional loss of data, such as tapes or disks lost in transit.

"The risk to consumers and businesses varies considerably, based on the type and scope of the data breach, which is why we think assessing the degree of risk for a given breach is critical in determining the best next steps," said Mike Cook, ID Analytics' co-founder and vice president of product.

ID Analytics said technology can measure the risk of a breach and distinguish which sets of breached data are used to commit fraud.

Identity-level breaches post the greatest harm for businesses and consumers due to fraudsters' sophisticated methods for profiting from identity information.

The calculated fraudulent misuse rate for consumer victims of the breach with the highest rate of misuse was 0.098%--fewer than one in 1,000 identities.

The reason for the minimal use of stolen identities: It takes time to actually perpetrate identity theft against a consumer, the company said. It takes roughly five minutes to fill out a credit application. At that rate, a fraudster--averaging 6.5 hours a day, five days a week, 50 weeks a year--would invest more than 50 years to fully use the breached file consisting of one million consumer identities.

If the criminal outsources the fraud work at $10 an hour to use a breached file of the same size in one year, it would cost the fraudster about $830,000, said the research report.

In certain targeted data breaches, notices may have a deterrent effect. In one large-scale identity-level theft, thieves slowed their use of the stolen data for identity theft after public notification of the breach.

The research also showed frausters used identity data manipulation or "tumbling" to avoid detection and prolong the scam.

"Consumers need to know the level of risk that is posed if they are part of a data breach. While any data breach is cause for concern, consumers that have been impacted need guidance as to the degree of risk involved," said Linda Foley, executive director of the Identity Theft Resource Center. "It's not helpful for consumers to receive a generic letter in the mail telling them they may or may not be at risk. We need to help victims of breaches understand when they need to be more vigilant and prevent them from being unnecessarily alarmed."

Resource Links
ID Analytics Inc. -