

RHR Information Services, Inc

SelectSmart News

Lawmakers Examine How to Ensure Privacy

Special points of interest:

- Feature Product: Social Security Number Trace
- The Information That Got Away
- Lawmakers Examine How to Ensure Privacy
- Types of Criminal Search Work

With all of the security breaches involving consumer data, Congress is starting to look at ways to ensure privacy rights. Last week, lawmakers confronted the executives of many of the companies where breaches have taken place. When executives responded with apologies and business practice changes, Congress started forming policy proposals of their own.

Below are 3 ideas lawmakers are considering and a summary of each:

Notification: This is a federal notification standard modeled on the California notification law. A similar measure failed

in 2003. The California law requires notification whenever a name and one other piece of data, such as a driver's license or credit card number, are compromised. Lobbyists are arguing for a narrower definition that only requires the companies to issue a notice when a breach poses a significant risk to identity theft. Executives at some companies would like Congress to leave the issue of when to notify "to the discretion of the institution", which leaves privacy activists angry. "I don't trust these guys to make the decision on when there's a real breach," said Ed Mierzwinski, of US Public Interest Research Group. Other bones of contention in-

clude how quickly a company must notify consumers, and whether an e-mail or website posting is enough. Several states are entertaining ideas on notification laws of their own.

Regulation: This idea would give the Federal Trade Commission authority to directly regulate data brokers. A Senator and a Representative have proposed legislation that would require the FTC to write and enforce guidelines for safeguarding information. A separate bill proposed by another Senator would compel a high-ranking executive to certify company compliance with the guidelines put forth by the

(Continued on page 3)

Inside this issue:

- The Information That Got Away **2**
- Feature Product: SS Number Trace **2**
- Criminal Search Work Types **2**

Editor's Note

We hope your first quarter of business in 2005 was good to you. Since implementation of our system enhancements we have heard good things from many of our customers. Look for more system upgrades that will make our system easier than ever to use!!

This month there are a lot of interesting stories on all of the recent data thefts and what Congress is doing to protect the consumers. Also, check out our featured product, the Social Security Trace Plus. This is the backbone of any SelectSmart package and returns

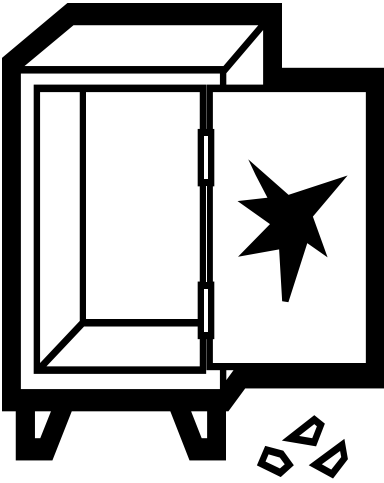
great basic information.

As always, if you have any questions or ideas on newsletter stories please feel free to contact us!

Elizabeth Army

Client Relations Coordinator

The Information That Got Away



Recently a series of news articles concerning the theft of consumer data from data brokers has raised serious issues concerning the privacy of consumer data. According to the Associated Press, a major national data firm recently began to notify about 145,000 Americans that their Social Security Numbers and other personal information may have been viewed by criminals posing as legitimate customers. In other recent

news, another large database company states that hackers commandeered one of its' databases, gaining access to the personal files of as many as 32,000 people. Also, backup files with data on more than 1 million customers of a national bank were lost. Further, credit card information on 100,000 customers was taken from the databases of a large retailer.

“security breaches”, besides the possible litigation, is that at least one of these data brokers has discontinued the sale of products that contain sensitive information, except where there is a customer driven transaction or benefit, or to local government for criminal justice purposes. Interestingly, in several cases it appears that the area of the businesses where the data was stolen from is where the

The result of these recent

(Continued on page 4)

Feature Product: Social Security Number Trace

“This product can be used for application reconciliation but will also drive your criminal search area.”

The Social Security Number Trace product is really the foundation for any package here at RHR Information Services, Inc. This product can be used for basic application reconciliation but also to drive your criminal search areas.

The information returned includes 1) any and all SSN's used by the applicant to obtain credit,

2) the number of times each SSN has been used, 3) any and all AKA's an applicant has used to obtain credit and 4) a 10 year address history.

This information is very important to obtain accurate criminal information. Criminal records are matched by name and date of birth, so it can be very important to know all aliases used by an appli-

cant. Also, criminal searches are usually requested on a state by state or county by county basis. If an applicant does not disclose previous addresses, the employer may not ever know they resided in another place. This is a common way many people hide past criminal convictions.

Contact your RHR / SelectSmart Rep for more information.

Which type of criminal search is best?



Criminal record searches are the most requested and considered by many, the most important product of a pre-employment background check. With many companies offering Instant Nationwide checks and other misleading products it is important

for the client to really understand these products and the type of information they contain.

Criminal records are generally kept and verified by name and date of birth, not the Social Security Number that some may believe. It is important to pair

your criminal product with one that verifies identity. These types of products will usually provide all AKA's a person may have used and also, a 10 year address history.

(Continued on page 3)

Criminal search, continued

(Continued from page 2)

Most criminal records in the US are kept in 3 different places: at the county courts, at statewide criminal repositories and at federal district courts.

County Courts

The county courts are the originating point for most criminal records and are typically more up-to-date than records at the state level. The disadvantage to a search like this is that it is limited to a single county. Because a person can be convicted of a crime in counties other than where they reside the scope of this criminal search is not very large.

State Repositories

All states keep a statewide repository for criminal records. Some states keep these repositories closed to anyone but law enforcement and others are extremely expensive or can take up to 3 months for the information to be returned. This product allows the client to view all

criminal offenses in the state on a prospective employer. Because counties are slow to report and then provide incomplete records a statewide search may not be as in depth as needed or wanted by a client.

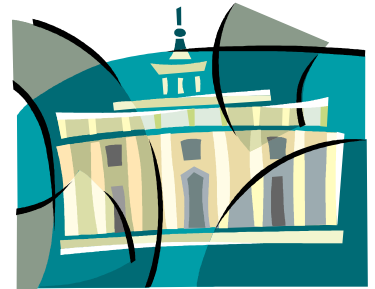
Federal Courts

The Federal criminal product will check the district courts of a specific state. The downfall with this product is two-fold. Some companies will charge for each district and states can have up to 4 districts. Also, a federal district court will not have records of offenses at the state level, they will only have records on Federal level crimes such as, robbery, drug trafficking and most white-collar crimes. It can be dangerous to use this product as the only criminal search performed.

Many companies are offering inexpensive instant nationwide database searches. Most often this is a search of available databases in the states from various

sources. Most often these sources are prison or inmate records or arrest records. Although this product can be valuable when paired with others, it is not recommended that it be the sole criminal search conducted. Because it is a database and usually a name match only, there are errors and omissions caused by inaccurate or incomplete data. As a result, a person with a serious criminal record can be shown as having no record and people with no criminal record can be shown to have extensive or serious records.

There is no single source of accurate and up-to-date criminal information currently available. The best way to develop your screening processes and determine which products you will use is to make sure you talk with a reputable screening company and educate yourself. Make sure that you understand the differences in the products and as always, Ask Questions!!



“There is no single source of accurate and up-to-date criminal information currently available.”

Lawmakers, continued

(Continued from page 1)

FTC. Business groups are against these types of guidelines. They say that bringing data brokers into a regulatory system could hinder police work and drive up the costs of verifications for businesses.

Credit Freeze: Advocates are urging Congress to look at another issue: How easy is it for identity thieves to open up new accounts using the fraudulent information? Like the Do-Not-Call Telephone List, advocates argue for a Do-Not-Issue-Credit List.

This list would enable a consumer to put a “freeze” on their credit history, preventing thieves from obtaining credit. Texas and California have already passed similar legislation and 20 other states are considering it.



10505 Wayzata Boulevard
Suite 200
Minnetonka, MN 55305

Phone: 888-389-4023
Fax: 888-389-4024
E-mail: earmy@rhris.com



The Right Path to the Right People



Disclaimer: This newsletter has been developed for informational purposes only for use by the customers of RHR Information Services, Inc., and should not be relied upon as definitively accurate. Due to the complex nature of employment law, we strongly suggest that you work closely with legal council when making employment related decisions.

Information, continued

(Continued from page 2)

companies supply data *without* the consent of the individual on whom the information concerned.

SelectSmart (a division of RHR Information Services, Inc) does not act as a data warehouse or sell consumer information to any unauthorized third party. This means that we only conduct searches on consumers that have signed a release and only release the information to the appropriate party. When an employer works with RHR Information Services, Inc. and

requests information on a prospective employee, the request is governed by the Fair Credit Reporting Act (FCRA) requirements. The employer must receive the applicants' consent in writing before we will perform any search or report any information.

It is because of our desire to protect the consumers' privacy and the confidentiality of our consumer data, that for someone to become a client and utilize our services, they will go through a required screening done by us to establish that the

client is a legitimate business with a need for access to confidential data. We at RHR Information take the responsibility of this business seriously and do all we can to protect ourselves, our clients and consumers from privacy violations.