

## EFFECTIVE BACKGROUND CHECKING VS TODAY'S SECURITY ENVIRONMENT

### IDENTITY THEFT AND DATA SECURITY CONCERNS AFFECT ACCURATE, RELIABLE BACKGROUND CHECKING

Business and personal records, or copies of them, are now routinely stored and accessed electronically, causing two competing concepts to come into direct conflict. How these opposing needs are managed will affect both our business practices, and personal lives.

The media are reporting increasing instances of a serious crime: *Identity Theft*. The FBI reports this is the fastest growing criminal enterprise in the country. To 'steal' someone's identity, a thief obtains sufficient current personal details to convince others he or she is that individual. Name, address, date of birth, Social Security Number, and driver's license or credit / bank account numbers are normally required.

The victim's identity is assumed long enough to defraud banks and other organizations, leaving the victim the monumental task of clearing their name and cleaning up the mess. The needed data can be acquired in many ways:

- ◆ Mail stolen from mailboxes
- ◆ Picking through garbage for discarded, intact financial records
- ◆ Phony email scams
- ◆ Phishing sites on the Internet
- ◆ Lost or 'misplaced' computers or storage devices
- ◆ Penetrated or 'hacked' computer networks.

Because of the frequency and severity of the crime, there is no doubt existing precautions to prevent loss of sensitive data should be rigorously enforced, and new safeguards developed. The importance placed on the problem is demonstrated by the increased federal, state and local regulations detailing how personal, identifiable data are to be used, stored and ultimately destroyed. We each need to be aware of protecting our own records, and as employer representatives, carefully guarding employee data.

The first solution often proposed to combat Identity Theft is to limit the information stored in databases to the extent that if a loss occurs, the data are not adequate to assume another's identity. Masking or deleting ID data can accomplish this. At first blush, this resolution makes a great deal of sense.

On further review, however, it raises a new area of concern and an equally troubling problem: *not being able to determine that a job applicant is a dangerous criminal*. Presently, a thorough background check is the primary tool used to screen potential employees. *However, preparing effective background checks depends upon using the sensitive data many want to make inaccessible*. This conflict may result in two opposite outcomes in Criminal Record research for a background check: reporting *no hits* because there is not an exact ID match, or reporting *numerous possible hits* for the same reason. Obviously, neither of these two results is of benefit to someone who wishes to make use of an effective screening tool.

There is no serious argument against the need for reliable, accurate background checks. A frequently cited reason is to keep violent, predatory individuals away from vulnerable persons, such as children, and the elderly. But that is only one illustration:

- ◆ A person should not have to fear that the repair technician in their home might be a threat to their family, their property or themselves.
- ◆ A shopper should not have to wonder if the employee taking them to the back of the store, where the product asked about is shelved, is a sexual predator, or has a history of violence.
- ◆ We should be able to have a reasonable belief that the person next to us at work has not been convicted of assault, is not a drug abuser, and does not have a history of harassment.
- ◆ An employer should not have to face the dilemma of whether to hire or reject a job applicant based upon a background check that shows only 'possible' convictions for assault, drug use, theft and embezzlement.

Therein lies the challenge: how can we protect privacy, prevent Identity Theft, and still allow access to critical data required for accurate background checks? It is not realistic to think that one of these important objectives should be attained totally at the expense of the other. The solution, then, is a question of balancing priorities: finding a set of guidelines and procedures that meets both needs.

There are a number of reasonable steps that can be taken on the security side of the equation:

- ◆ More robust data encryption in electronic storage media
- ◆ Better firewalls on computers, computer networks and the Internet
- ◆ Establishing and enforcing rules regarding removal or copying of database information
- ◆ More stringently enforced procedures for access to and transfer of data
- ◆ Selective use of truncation of identifying data
- ◆ Not collecting and storing ID information that is not essential to the purpose
- ◆ Proper encryption when electronic transmissions occur

It is important to recognize the difference between protecting data from curious or malicious eyes, and making it available to those with a legitimate need. People who are unaware of the importance of accurate background checks often overlook this distinction. Court systems, DMV's, and others, sometimes in response to legislative measures, have begun to limit the identifiable data they expose, or to arbitrarily restrict access to data. Some take the stance that partially masking information is not sufficient, and data is being purged altogether. Many also take the position that they do not want to

have to decide who has a legitimate need for access, and who does not. If data is denied to all, they are content to believe they are erring on the side of 'safety.'

It may not be possible to reverse this trend, at least in the short term. Therefore, those of us who prepare, and those of us who order and use background checks, must take steps to offset the effect of only partial ID data. Instead of having one or two complete, matching points, we may have to rely on finding several partial matching points, accumulating enough 'possible' matches to turn the situation into a positive match. *The most effective procedure we can use to accomplish this is to be sure we have complete applicant data.* That means:

- ◆ Providing full legal names, not partial names, nor initials, nor nicknames
- ◆ Providing any previous legal names used within the applicable research time frame
- ◆ Ensuring we have an accurate Social Security Number
- ◆ Providing a complete date of birth
- ◆ Providing a complete driver's license number
- ◆ Providing an address history of reasonable length to cover the applicable research time frame

There are more than 6,000 criminal courts in the US. The methods of accessing their records vary greatly. Some court systems maintain records in county-wide or state-wide databases; many do not. These databases, especially those in large metropolitan areas, have grown so large, it is entirely unreasonable to assume anyone can, or would even attempt to sift through them with only partial ID data. All one need do is look at a metropolitan area telephone book, and count the number of times you can find a 'possible' match to someone whose name is 'William Smith,' or 'John Taylor' to see the enormous difficulty involved in searching with only partial information.

Providing a researcher with data in accordance with the above steps will allow the individual to first, limit possible hits that have to be researched further to a manageable few, and, in the end, show results that can confidently be associated with the applicant. Only in this way can the usefulness and viability of background checks continue to be a valuable tool for the HR professional.