5 Most Common Mistakes in Background Checks and How to Correct Them

Imagine that you finally land a dream job only to have it turned into a nightmare because false information found on your pre-employment background check prevents you from gaining employment. From entry-level to executive suite, most jobs these days require a pre-employment background check.

A recent survey from the Society for Human Resource Management (SHRM) revealed at least 80 percent of U.S. businesses conduct some variety of background checks on prospective employees, and many employers are re-checking current workers in addition to applicants.

Statistics also show that hiring managers find discrepancies on over 50 percent of applications and resumes. With high unemployment resulting in a large pool of talented job seekers, employers can - and most surely will - be as stringent as possible when it comes to the pre-employment screening process. If you're one of the millions of people who are currently looking for work, you most likely will undergo a background check.

What's in a Background Check?

The types of searches that are induced in background checks depend on-the-job, but the majority of them include:

- A Social Security Number (SSN) Address Trace to locate addresses you may have lived at
- Some type of criminal record search (county, state, U.S. Crim, or federal)

In addition, many employers seek other information such as:

- A sex offender search
- Anti-terrorist search
- Employment/salary verification
- Education verification
- Prfessional license verification
- Motor vehicle driving records (MVR) search
- Credit report (mostly in jobs dealing with finances and executive level positions)

To ensure that your personal information is correct, you need to know what possible mistakes, errors and inaccuracies are most common during a typical background check. Once found, they can be removed or changed. Here are 5 common mistakes found in background checks and why they occur.

1. Mistaken Identity

When you visit a social networking website - such as Facebook, Twitter or LinkedIn - are you surprised to discover that many other people share your name? Do some make you say "That's no the right (your name)! I'm me!" It shouldn't come as a shock that a subject of a background check can get mixed up with a less than desireable namesake. What's even more surprising, though, is the fact that most criminal record cases in the United States do not contain a social security number. As a result, courhouses use the name and date of birth as the main identifier. Therefore, it's very easy and common for the criminal record of another person to be returned that has your name, and in some cases, your birth date, as identifiers.

2. Incorrect Social Security Number

Your nine-digit social security number (SSN) is more important than your name because it's unique to you. However, a simple typo in one of the digits can lead to a wealth of trouble during a SSN Trace, which reports names and addresses used or associated with the number. It's often the first step in most background checks

3. Identity Theft and Fraud

Sometimes, it's no accident when another person ends up with your name and SSN. According to Javalin Research, identity theft increased 22 percent in 2008 and has victimized nearly 10 million U.S. adults. The unauthorized use of another person's personal information for financial gain is rapidly becoming a popular way to earn a living in today's economy. A criminal with your identity can commit crimes, get arrested, and skip a trail, leaving you with a warrant for your arrest.

4. Incomplete or Missing Information

Inaccurate and out-of-date information is bad enough, but sometimes your records contain incomplete or missing information that fails to tell employers the whole story about a criminal background. Most experts agree that upfront communication about any criminal record is the best practice to pursue. Most background checks do not contain all of the information in a criminal file - only partial information gleaned from a quick glace or electronic look-up of the record. Items such as dismissals, expungement, deferred adjudication, diversion programs, or successful completion of parole or probation may be left out in error. So, it's important to make sure the prospective employer knows all of the facts, including a criminal history.

5. Illegal Information

Many states have protections on what information may be included in a background check or how it's procured. For example, the states of California, Nevada and New Mexico limit the number of years back your background check report may go to a maximum of 7 years. Others - such as Kansas, Maryland, Massachusetts, New Hampshire, New York and Washington - allow the use of criminal records going back more than 7 years if the proposed salary is above a specific amount ($20,000 - $25,000 per year, depending on the state). Some states even restrict the types of records that may be reported. For example, California limits reporting marijuana convictions over 2 years from the date of reporting.

On a federal level, the use of some criminal records in a hiring decision can be deemed discriminatory. For more information, refer to the U.S. Equal Employment Opportunity Commission guidelines on the use of criminal records.

Finally, the biggest issue is when background checks are performed without the applicant's written consent. All employers must request permission from the applicant or employee before running a background check through a third-party agency. This is a federal law that cannot be preempted by any state law.

Correcting Errors Found on Background Checks?

The law is usually on the applicant's side when it comes to background checks for employment purposes. Prior to making a decision not to hire you, the employer must provide written notice of their intent to do so and the name of the background check company they used to collect information on you.

A copy of the report must be provided to you, and the employer must wait at least 5 days to allow you the opportunity to dispute the information within the report. If an error is indeed found and it's disputed, the employer and the background check company must reinvestigate the dispute, make any necessary corrections and provide proof to you that they've taken these steps.

Avoiding Background Check Errors

Job seekers can avoid errors by ensuring their information is current, accurate and secure with a "personal" background check. Conducting a background check yourself initially will give you a sense of what personal information is on record for you and give you the chance to review it for any discrepancies or inaccuracies.

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is personal information such as name, social security number (SSN), birth date, driver's license number and brith certificate.. From birth to death, every person leaves a trail of PII. It's up to consumers to ensure their Personally Identifiable Information (PII) is correct with a personal background check.

The Federal Identity Theft & Assumption Deterrence Act of 1998 states that a person's PII - or "means of identification" - may also include alien registration number, government passport number, employer or taxpayer identification number, unique biometric data (fingerprint, voice print, retina or iris image), a unique ectronic identification number, address, routing code and telecommunication identifying information.

Everyone has PII and is vulnerable to foreign privacy laws, or lack thereof, and should monitor that information as frequently as possible to expose bad practices, lessen the risk of identity theft and increase data privacy and security. With so many forms of PII and their prolific use in everyday life, the risk of identity theft is much greater, which makes security data privacy even more difficult.

WHY PII Should Be Protected

According to reports from the Society of Human Resource Management (SHRM), more than 80 percent of U.S. businesses currently perform some form of pre-employment background check before the actual hire of a prospective employee.

Typical background checks consist of applicants voluntarily giving away their PII - everything needed to steal an identity. What most people fail to realize is the likelihood that much of the PII collected during a background check travels far beyond the security of U.S. privacy laws to a foreign call center or data warehouse with little to no standards for privacy protection. How could this happen?

In today's digital age, most information gathered during the recruitment and hiring process is stored electronically. For employers, Applicant Tracking System (ATS) software applications assist in the management of resumes and applicant information while enabling the electronic handling of recruitment and talent management needs. Meanwhile, an online Job Board System (JBS) where prospective employees use an Electronic Application Process (EAP) helps to match qualified candidates with the right jobs quickly, easily and successfully.

The protection of PII electronically collected through these methods should be of the utmost importance to any company. This whitepaper focuses on the data privacy and security of PII - specifically regarding of shoring, repurposing and reselling when used in the background screening industry, ATS and JBS, along with all aspects of everyday life - personally and professionally.

Data Security and Privacy

Data security is the means of keeping data safe from corruption and suitably controlling access to that information, helping to ensure data privacy and protect personal data. Data privacy is the relationship between collection and dissemination of data, technology, the public expectation of privacy and the surrounding legal and political issues. Privacy concerns exist wherever PII is collected and stored. Improper or non-existent disclosure control can be the root cause for privacy issues. Data privacy issues can arise in response to information from a wide range of sources, including:

- Healthcare records
- Criminal justice investigations and proceedings
- Financial institutions and transactions
- Biological traits (i.e. genetic material)
- Residence and geographic records

The challenge facing businesses today in the field of data privacy is how to share data when necessary, while at the same time protecting each individual's PII through effective data security and information security design.

Identity Theft

Growing popularity of offshoring, repurposing and reselling PII and services has led to identity theft and loss of privacy. In recent years, offshore call center workers have defrauded U.S. bank customers, and identity theft gangs have sold thousands of offshored credit card and passport data for as little as $5 each. As a result, many states have taken measures to prevent the misuse of PII in order to fight the rising tide of identity theft. Because of this, the federal government has taken action with the Gramm-Leach0Billey Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The FCRA also provides additional protection against identity theft.

Unfortunately, protection against identity theft ceases to exist once PII is sent overseas. While some countries outside of the U.S. have strong data and privacy protection laws, - such as the European Union (EU) states - many places where information is sent offshore for processing have little or no practical identity theft protection. However, they offer a way to cut costs. American citizens are unable to enforce their privacy rights overseas. It's neither practical nor cost-effective to access foreign courts, contact foreign police, lodge a complaing, or obtain assistance about identity theft. The lack of any meaningful protection once U.S. data is sent offshore is a major hurdle in the effort to combat identity theft and to protect privacy.

Identity theft continues to grow and thrive. The 2009 Identity Fraud Survey Report by Javelin Research revealed that the number of identity fraud victims has increased 22 percent to almost 10 million adults in the U.S. Approximately 1.8 million more adults were victimzed by identity fraud in 2008 than the previous year - the first year-over-year increase since Javeline Research began collecting data.

Offshoring, Repurposing & Reselling PII: How Could They Do That?

How could a company send a U.S. citizen's Social Security number (SSN) overseas without the permission of its rightful owner? Because many background screening companies and ATS/JBS providers choose to ignore the dangers of identity theft and loss of data. l and continue to resell, repurpose, and offshore the PII of clients for data entry without their knowledge or consent. In this time of heightened security, such activities are a great risk to the personal privacy and personal data of U.S. citizens. Companies should consider more than just lower costs and this critical for clients to know that a slew of security exposures could be included with offshoring.

Unfortunately, all protections against identity theft as a practical matter cease to exist once offshoring sends data out of the U.S. Some countries outside of the U.S. have strong data and privacy protection laws. However, many countries have little or no practical identity theft protection. These countries are selected for offshoring because they offer a way to cut costs. It's difficult for a U.S. consumer to contact foreign policy to lodge a complaint about identity theft or to obtain assistance.

Privacy Laws

Privacy is a central element of the Federal Trade Commission's (FTC) consumer protection mission. Advances in technology make it possible for detailed PII to be compiled and shared cheaper and easier than ever. While these advances have produced many benefits, when PII becomes more accessible, companies, associations, government agencies, and consumers must take precautions to protect against the misuse of information. A key part of the Commission's privacy program is to make sure companies keep promises made to consumers about privacy, including precautions taken to secure consumers' personal information. In response to concerns about privacy, many Websites post privacy policies that describe how consumers' personal information is collected, used, shared and secured.

Federal Trade Commission Act

Using its authority under Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the market place, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises aboutthesecurityofconsumers'personalinfomation.The Commission also used its authority to challenge information practices that cause substantial consumer injury. Under this Act, the Commission is empowered, among other things, to conduct investigations relating to the organization, business, practices, and managementof entities engaged in commerce.

Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act is enforced by the Federal Trade Comission (FTC) and promotes accuracy in consumer reports and is meant to ensure the privacy of information within them. The FTC educates consumers and businesses about the importance of personal information privacy and security. Under the Act, the Comission guards against unfairness and deception by enforcing companies' privacy promises about how they collect, use and secure consumers' personal information.

Companies that gather, assemble and sell personal information are called Consumer Reporting Agencies (CRA). The most common type of CRA is the nationwide credit bureau such as Experian, Equifax and Trans Union. Other types include employment screening services that offer reports on consumers and are also governed by the FCRA. CRAs may sell information to creditors, employers, insurers and others in the form of a consumer report. To be covered by the FCRA, a report must be prepared by a consumer reporting agency - a business that assembles reports for other companies, such as a background check company. Background screening companies have a legal obligation to keep this information secure when it's in their possession.

Many states have passed laws or regulations to protect their citizens. In addition to complying with federal laws, businesses should look to state laws to make sure they're compliant. Despite these different rules, the FTC has tried to develop a single basic standard for data security that strikes the balance between providing concrete guidance and allowing flexibility for different businesses' needs. The standard is straightforward: companies must maintain reasonable procedures to protect sensitive information.

The Gramm-Leach-Billey Act (GLBA)

The financial Modernization Act of 1999, also known as the Gramm-Leach-Billey Act or GLBA, includes provisions to protect consumers' personal financial information held by financial institutions. There are two principal parts to the privacy requirements:

- The Financial Privacy Rule governs the collection and disclosure of customers' personal financial information by financial institutions. It also applies to companies, whether or not they're financial institutions, who receive such information.
- The Safeguards Rule requires all financial institutions to design, implement and maintain safeguards to protect customer information and applies to financial institutions that collect data from their customers, and financial institutions (like CRAs) that receive customer information from other financial institutions.

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA), also known as the Kennedy-Kassebaum Health Insurance Portability and Accountability Act, was enacted by the U.S. Congress in 1996. Under HIPAA, someone with individually identifiable health information should have established procedures for individual health information privacy rights, and the use and disclosure of individual health information should be authorized or required.

Employment Enhancement

Background checks have been performed by employers on prospective employees for years. Jobseekers requesting background checks on themselves in order to better their chances of getting hired is a recent development. By giving yourself a personal background check, you're taking control of your own personal information - a good idea no matter what your employment situation is - and telling prospective employers that you have nothing to hide.

About Pre-employ

Headquartered in Northern California, Pre-employ is a national leader in the screening industry. For more than 20 years, Pre-employ has provided cost-effective solutions that deliver quality employee background screening services, industry best practices, and valuable resources to help minimize risk and enhance the hiring process. For two years in a row, Pre-employ was named to Business News Daily's Best Background Check Services.

For more information, please visit www.pre-employ.com.

The Nation's #1 Background Check Company

- Superior turnaround times
- Quality customer service
- Accuracy with full transparency
- Best price guarantee