
The Five Most Common Mistakes In Background Checks

& How to Correct Them

A FREE Guide from MyBackgroundCheck.com



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

Introduction

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 jobseekers, employers can – and most surely will – be as stringent as possible when it comes to the pre-employment screening process.

If you are one of the millions of people currently looking for work, you most likely will undergo a background check.

What's in a Background Check?

The types of searches that are included 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); and
- Some type of Criminal Record Search (county, state, 'US Crim,' or federal).

In addition, many employers seek other information such as:

- A Sex Offender Search;
- Anti-terrorist Search;
- An Employment/Salary Verification;
- An Education Verification;
- A Professional License Verification;
- A Motor Vehicle Driving Records (MVR) Search; and
- A Credit Report (mostly in jobs dealing with finances and executive level positions).



The Five Most Common Mistakes in Background Checks

To ensure that your personal information is correct, you need to know what possible mistakes, errors, and inaccuracies are most common during typical background checks. Once found, they can be removed or changed. Here are the “Five Common Mistakes in Background Checks” and the reasons they occur:

COMMON MISTAKE #1: Mistaken Identity

When you visit a social networking website such as Facebook, MySpace, or LinkedIn, are you surprised to discover that so many people share your name? Do some make you say: “That’s not the right (your name)! I’m me!” So it shouldn’t come as a shock that a subject of a background check can get mixed up with a less than desirable namesake. What is surprising though is the fact that most criminal record cases in the United States do not contain a Social Security Number. As a result, courthouses use a name and date of birth as the main identifier. So it is very easy and common for a criminal record of another person to be returned that has your name, and in some cases, your date of birth, as identifiers.



COMMON MISTAKE #2: Wrong Social Security Number

Your nine-digit Social Security Number (SSN) is more important than your name, since no one is allowed to share your SSN number (unlike your name). But a simple typo in one of those nine digits can lead to a lot of trouble during the SSN Trace, which is usually the first step in most background checks, and reports any names and addresses used or associated with the SSN, and if the SSN belongs to a deceased person.

COMMON MISTAKE #3: Identity Theft & Fraud

Sometimes it is no accident when someone else ends up with your name and your SSN. Identity theft increased 22 percent in 2008 to victimize almost 10 million U.S. adults, according to a report released by Javelin Research. The unauthorized use of another person’s personal information to achieve financial gain is rapidly becoming a popular way to earn a living in today’s economy. A criminal with your identity can commit crimes, be arrested, and skip a trial, leaving you with a warrant for your arrest.

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

COMMON MISTAKE #4: Incomplete & Missing Information

Inaccurate and out-of-date information is bad enough, but sometimes your records contain incomplete or missing information that fails to tell “the whole story” – i.e. the truth – which means that you will have some explaining to do after a background check. “It wasn’t my fault...” and “What really happened...” are two phrases that you never want to have to say during a job interview. Most experts agree that up front communication about any criminal record is the best practice to pursue. Many background checks do not contain all of the information in the criminal file, only partial information gleaned from a quick glance or an 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. It is important to make sure the prospective employer knows all of the facts, including how it all ended.



COMMON MISTAKE #5: Illegal Information

Many states have protections on what information may be included in a background check or how it is procured. For example, California, Nevada, and New Mexico (in most cases) limit the years your background check report may go back to a maximum of seven (7) years. Other states (Kansas, Maryland, Massachusetts, New Hampshire, New York, and Washington for example) allow the use of criminal records beyond seven (7) years if your proposed salary is above a certain amount (some are \$20,000 a year and others \$25,000 per year, depending on the state). Some states even restrict the types of records that may be reported (California limits reporting marijuana convictions over two years from the date of reporting, for example). On a federal level, the use of some criminal records in a hiring decision can be deemed discriminatory (Find U.S. Equal Employment Opportunity Commission guidelines on the use of criminal records at www.eeoc.gov/policy/docs/convict1.html).

The biggest legal issue is if you discover an employer conducted a background check on you without your written permission. All employers must receive your permission before procuring a background check through a third party agency. This federal law cannot be preempted by any state law and must be followed.

How Do I Correct Any Errors Found on Background Checks?

You’re in luck. The law is on your side when it comes to background checks for employment purposes. Prior to making a decision not to hire you, the employer must give you written notice of their intent to do so and the name

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

of the company that conducted the background check on you. They must also give you a copy of the report and wait at least five (5) days to allow you to dispute the information in the report. If an error is found on the report and you dispute it, the employer and the background check company must reinvestigate the dispute and correct any errors and prove to you that they have done so.

How Can I Avoid Errors on Background Checks in the First Place?

Jobseekers can avoid errors on background checks by making sure their information is current, accurate, and secure with a “personal” background check. In today’s “Age of Information,” people are what their personal information says they are. Jobseekers consenting to a background check should at least know what information will be uncovered beforehand or else suffer the consequences of lost jobs. Personal background checks protect consumers by protecting their personal information and finding any errors before they find the consumers. Since it is their information, it is up to consumers to make sure their Personally Identifiable Information (PII) is correct with a personal background check.

What is Personally Identifiable Information (PII)?

From birth to death, everyone leaves a trail of Personally Identifiable Information (PII), from a birth certificate to a death certificate. What exactly is PII? The most recognized forms are: name, Social Security number (SSN), birth date, driver’s license number, and birth certificate.

The Federal Identity Theft & Assumption Deterrence Act of 1998 states that a person’s PII – or “means of identification” – may also include any of the following: alien registration number, government passport number, employer or taxpayer identification number, unique biometric data (fingerprint, voice print, retina/iris image), a unique electronic identification number, address, or routing code, and telecommunication identifying information or access device.

Since everyone with PII is vulnerable to foreign privacy laws, or lack thereof, PII should be monitored as frequently as possible to expose bad practices, lessen identity theft risk, and increase data privacy and security. With the many forms of PII, and their prolific use in everyday life, the risk for identity theft is much greater and attaining data privacy more difficult.

Why Should PII 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.

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

Typical background checks consist of applicants voluntarily giving away their Personally Identifiable Information (PII) such as name, birth date, and Social Security number (SSN) – basically, everything needed to commit identity theft. 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 Personally Identifiable Information electronically collected with background screening, ATS, and JBS should be of the utmost importance to any company collecting PII. This white paper focuses on the data privacy and data security of PII – specifically regarding offshoring, repurposing, and reselling when used in the background screening industry, ATS, and JBS, and also all aspects of everyday life, both personally and professionally.

Data Security and Data Privacy Defined

Data security is the means of keeping data safe from corruption and suitably controlling access to that information, thus helping to ensure 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, such as:

- Healthcare records;
- Criminal justice investigations and proceedings;
- Financial institutions and transactions;
- Biological traits, such as genetic material; and
- 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 very same time – protecting each individual's PII through effective data security and information security design.

Identity Theft

The growing popularity of offshoring, repurposing, and reselling of PII data and services has led to identity theft and lost 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 details for as little as \$5.00 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. The federal government has taken action with the Gramm-Leach-Bliley Act (GLBA) and Health Insurance Portability and Accountability Act (HIPAA) of 1996. The Fair Credit Reporting Act (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 is neither practical nor cost-effective to access foreign courts, contact foreign police, lodge a complaint, 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., and approximately 1.8 million more adults were victimized by identity fraud in 2008 than in 2007, the first year-over-year increase since Javelin began collecting data.



Offshoring, Repurposing & Reselling PII: Why Would They Do That?

Why would a company offshore or resell personal and secure data without permission from the rightful owner? The obvious reason – besides the fact that it is easy to do and saves money (at least initially) – is that the rightful owner of the information does not even have to be notified.

With the rash of highly publicized data breaches in the news, many states now have their own disclosure laws mandating companies to inform clients of actual or suspected security breaches, and also of data breaches occurring overseas when sensitive PII is sent offshore.

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

What is Data Offshoring and Data Repurposing?

Offshoring, or offshore outsourcing, is the business practice of transferring jobs, services, and personal data to low-cost labor markets by using companies internationally to increase profits. While offshoring may help some U.S. background check firms and ATS/JBS providers lower costs, these activities bring great risk to the PII data of U.S. citizens in the form of identity theft.

Repurposing, in regards to the PII of individuals, refers to the use or conversion of use in another format or product, such as marketing purposes. The PII data can also be resold to skip tracers, lawyers, data aggregators, or marketing lists to be bought and sold again and again.

Reasons for Offshoring, Repurposing & Reselling Data

Many large U.S. background check companies increase profits by routinely engaging in offshoring, repurposing, or reselling PII without telling clients or applicants. In recent years, U.S. citizens have greatly benefitted from cost lowering services by outsourcing overseas. However, the lowered prices come at the cost of risking data privacy and security.

Large screening firms engage in offshoring PII in bulk on a daily basis in order to lower their operating costs and increase profits. Increased data reselling and data offshoring has resulted in State and Federal Government taking preventive measures to fight identity theft from the misuse of PII. While offshoring has grown in popularity as companies look to cut costs and increase profits, what are the costs to an individual's privacy?

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 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 it is critical for clients to know that a slew of security exposures could be included with offshoring.



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

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 Web sites 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 (FTC) Act, which prohibits unfair or deceptive practices in the marketplace, the Commission has brought a number of cases to enforce the promises in privacy statements, including promises about the security of consumers' personal information. 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 management of entities engaged in commerce.

The Fair Credit Reporting Act (FCRA)

The Fair Credit Reporting Act (FCRA) – enforced by the Federal Trade Commission – promotes accuracy in consumer reports and is meant to ensure the privacy of the information in them. The FTC is educating consumers and businesses about the importance of personal information privacy, including the security of personal information. Under the FTC Act, the Commission 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 (CRAs). The most common type of CRA is the nationwide credit bureau such as Experian, Equifax, and TransUnion. Other CRAs, such as employment screening services that offer reports on consumers, 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



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

company. Background screening companies have a legal obligation to keep this information secure when it is 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 are in compliance. 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-Bliley Act (GLBA)

The Financial Modernization Act of 1999, also known as the Gramm-Leach-Bliley 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 are 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.

The 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. With HIPAA, an individual 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.



Offshoring, Repurposing & Reselling PII: How Dare They Do That!

How dare a company resell personal information! 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 is difficult for a U.S. consumer to contact foreign police to lodge a complaint about identity theft or to obtain assistance.

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 are 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. If you are willing to pay for new clothes, a new haircut, a resume-polishing, a job fair, an employment seminar, or a book on how to find a job, why not purchase a background check so you can see what potential employers will see BEFORE they see it?

MyBackgroundCheck.com

MyBackgroundCheck.com is a pioneer in consumer-requested background check services and one of the first to use a secure web-based ordering portal for individuals who wish to purchase a background check. We are a leader in the growing “Personal Information Management” movement and offer consumers control over their personal information, knowledge of who is viewing their reports, and a safe and easy way to share their information with anyone else they choose. To take control of your personal information with an account from MyBackgroundCheck.com, visit us at www.mybackgroundcheck.com.

