crimcheck.com™

HR Resources | Best Practices Series

5 STEPS To Ensure Compliance with the FCRA for HR

01 Employers Must Certify Certain Items to the Screening Company

02 Disclosure and Authorization

03 Pre Adverse Action Notification

04 Adverse Action Notification

05 Retaining and Disposing of Background Check Information

Compliance with the FCRA for Employers: Step 1

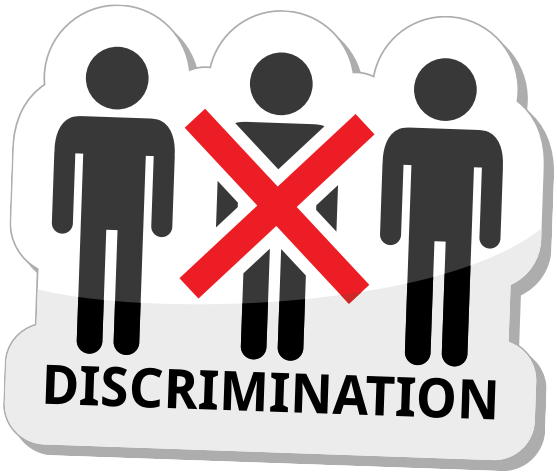
01

Employers Must Certify Certain Items to the Screening Company

Background checks have now become a critical part of the hiring decision making process. When making decisions like hiring, promotion, retention and reassignment, it is now customary for employers to order background checks. The common checks include employment history, education verification, criminal records, financial history and even social media usage.

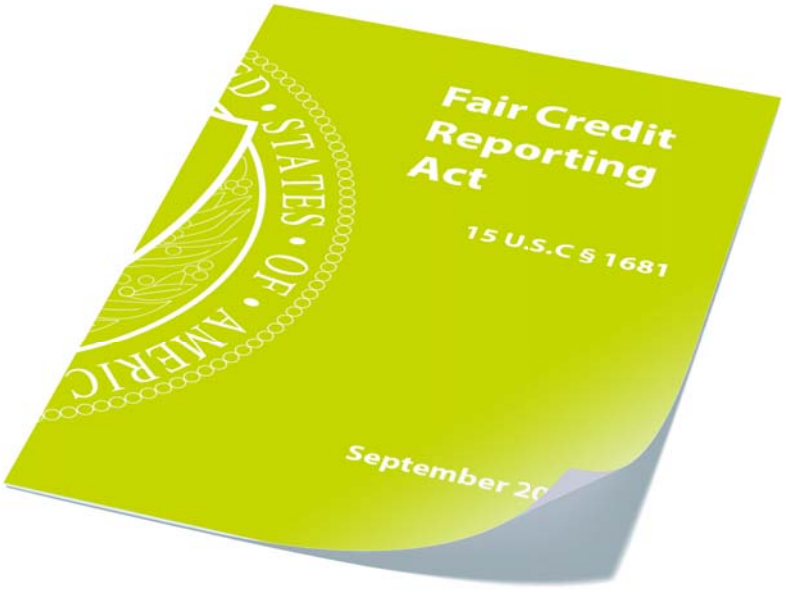
In most cases, companies contract third-parties (other companies which offer background checking services) to carry out the checks on their behalf. The information gathered from the checks often plays a critical role in influencing hiring decisions.

There are strict legal guidelines which govern how background screening may be carried out. Such guidelines govern what kind of information can be collected, the procedures for collecting the information, and how the information may or may not be used. If you intend to carry out background checks, you need to understand these legal guidelines.



For starters, no information that is obtained from a background check may be used to foster any form of discrimination. This includes discrimination on the basis of gender, race, color, religion, national origin, religion, disability, medical history (including genetic information) and age. Such discrimination would be a violation of laws such as Age

Discrimination in Employment Act (ADEA), Genetic Information Nondiscrimination Act (GINA) and others. Such laws are enforced by the Equal Employment Opportunity Commission (EEOC).



Secondly, if you intend to hire another company to carry out background checks on your behalf, then you need to know about the Fair Credit Reporting Act (FCRA). The FCRA is the law which governs background checks carried out by third parties. As such, FCRA compliance is essential if you intend your background checks to be carried out within the boundary of the law.

The first step towards compliance is understanding what the FCRA is, how it applies to background checks, and the guidelines it provides for carrying out background checks. We shall explore each of these aspects in detail later. For now, let's begin by looking at what the FCRA is.

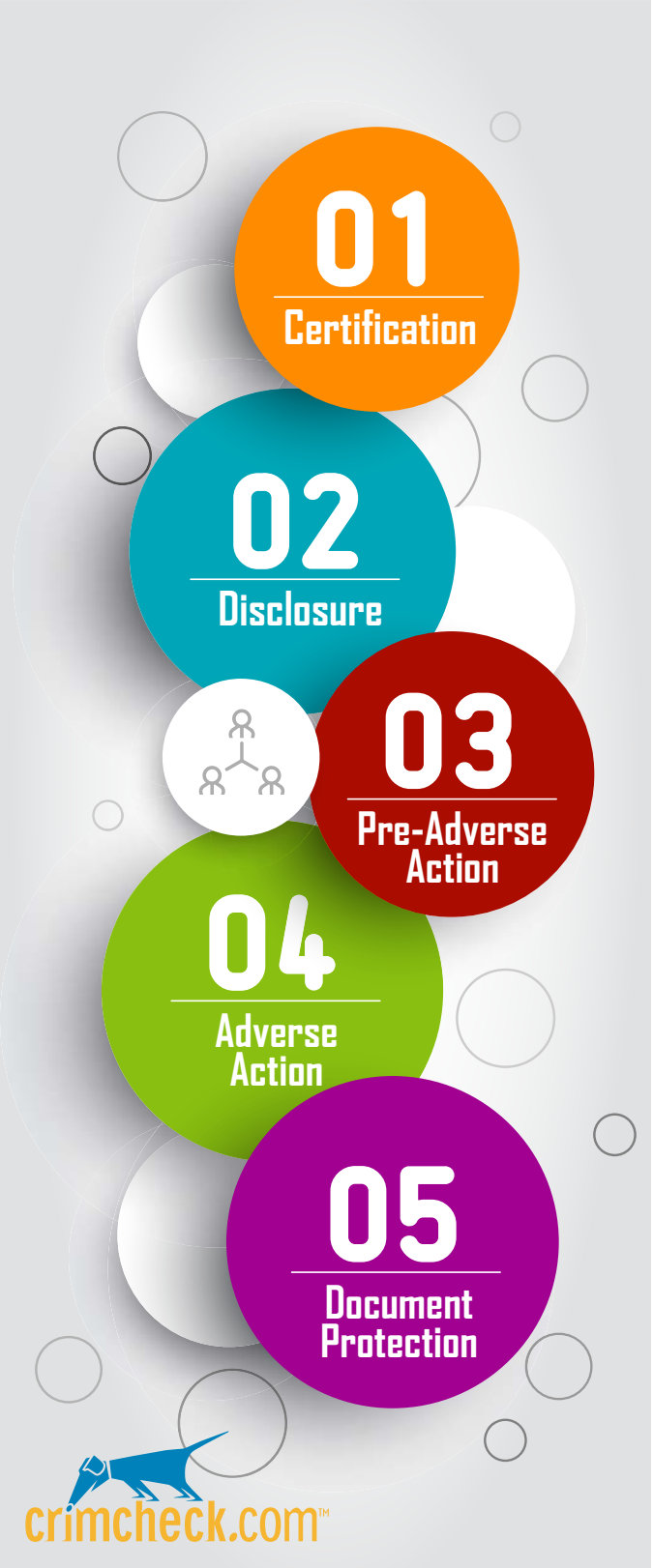
The FCRA is a federal law which regulates the collection, dissemination and use of consumer information. In some contexts, the FCRA governs credit information. However, in the context of hiring, it governs information contained in criminal background records, employment records and driving records, and any other information gathered to make an employment decision.

The FCRA specifically comes into play when the information is collected by third-parties. Such third parties are typically companies which specialize in offering screening services. In FCRA lingo, such companies are referred to as Consumer Reporting Agencies (CRAs). The information they collect is referred to as a consumer report.

The FCRA basically stipulates guidelines which govern the interaction between CRAs, employers (the ones who hired the CRA) and the employees or applicants (the ones on whom the background checks are being carried out).

In a nutshell, FCRA guidelines can be summarized into 5 simple steps. They are:

1. Employer certification to the CRA
2. Disclosure to and authorization from the applicant
3. Pre-adverse action Notice
4. Adverse action Notice
5. Document Protection and Destruction



In due course, we shall look at each of these steps in depth. For now, there are two important things to note about laws regarding background checks. The first is that although FCRA is a federal law, many states have their own FCRA laws which have slight variations from the federal law. As such, to be on the safe side, you need to understand the FCRA law for your specific state or jurisdiction.

Secondly, some states have their own consumer protection laws which were in place long before the enactment of FCRA. The FCRA doesn't invalidate these laws. As such, before starting to carry out background checks, you need to research any relevant laws in your jurisdiction.

The good news is that finding out about such laws is quite simple. Since you are reading about FCRA compliance, chances are high that you intend to hire a CRA to carry out background checks on your behalf. Any CRA worth their salt can point you in the right direction to locate any relevant laws in your jurisdiction. State, cities, and counties can all have their own legislation that covers hiring practices.

Anyway, our focus here is FCRA, so let's stick to it. Before you can order background information from a company, the FCRA provides guidelines to follow. The first thing you need to do is to send a written certification to the CRA.

You basically need to certify that your company:

- Notified the employee or applicant that you intend to carry out a background check on them.
- Obtained written permission from the employee/applicant to carry out the background check (Some CRAs request to see the written authorization).
- Will not use the information to discriminate against the employee/applicant, or to

willfully violate state or federal laws.

- Will comply with all FCRA requirements as regards the use and dissemination of the information obtained from the background check.
- That you have a permissible purpose for which the report is being obtained.

For example, FCRA stipulates a number of steps which have to be taken if the information collected will instigate an "**adverse employment action**." An adverse employment action is basically a decision which will result in unfavorable consequences for the applicant or employee. Examples include not getting hired, getting fired, getting demoted or having certain benefits slashed. Among the steps recommended by FCRA is a provision for the applicant/employee to challenge any findings in the background check.

The point here is that before commissioning a background check, you have to submit a written certification for to the CRA. The CRA will review the certification, and may ask for any relevant supporting documents (e.g. a written authorization from the applicant /employee). Once they are satisfied with your request, then you can proceed to discuss the necessary terms.

In a nutshell, background checks play an essential role in guiding hiring decisions. As such, most companies hire them out to third parties – companies which specialize in carrying out background checks. As soon as they do this, they come under the scope of the Fair Credit Reporting Act (FCRA). The FCRA is a law which stipulates how background information may be collected, disseminated and used.

As such, **every employer** needs to understand the provisions of FCRA in order to comply with them. In case you are an employer, the above information should

be a good introduction to FCRA. However, it is just the beginning. In subsequent posts, we will get deeper into other aspects of FCRA, beginning with disclosure and authorization.

FCRA Compliance: Step 2 02

Disclosure And Authorization

Disclosure and authorization is one of the easiest Fair Credit Reporting Act (FCRA) provisions to observe. It is also one of the easiest to violate; and its violations can be extremely costly. In fact, over the last two years, the hottest topics in class action lawsuits against employers have resulted from FCRA disclosure and authorization violations.

One of the most famous is the recent $3 million settlement reached in the Brown v. Delhaize America, LLC class action suit. This originated in March 2014 when Food Lion LLC, a Delhaize America LLC – owned company, background check procedures came into question.

The company was accused of violating the FCRA because of its lack of pre-adverse action procedures, and because their disclosure and authorization forms were not stand alone documents. The lawsuit claimed that the

employer took action against employees without providing those employees with pre-adverse action notices, thereby negating their chances to dispute information in background check findings.

The employee brought a lawsuit against Delhaize America – Food Loin's parent company – alleging violation of FCRA disclosure rules. She was soon joined by 59,000 other people who had applied to Delhaize-owned stores for the past two years. Realizing that it was in a no-win situation, Delhaize struck a deal with the plaintiff's lawyers to pay a $3 million settlement. **On 2nd March, 2015, the plaintiffs applied to the court to approve the settlement, and the court obliged**.

The Delhaize case is by no means an isolated one. It is just the latest settlement in a recent spate of class action lawsuits involving FCRA background checks. Another popular example occurred in October 2014. **In this case, Publix Super Markets Inc. paid out close to $6.8 million to settle a class action brought by 90,000 job applicants making claims about authorization and disclosure violations**.

The bottom line is that FCRA disclosures and authorizations can be a potential can of worms for an employer carrying out background checks. Failing to follow those guidelines can open you up to expensive and reputation damaging lawsuits.

The good news is that FCRA guidelines on disclosures and authorizations are quite straightforward. Observing them is so easy that it takes almost no effort. Employers who violate them usually do so out of mere lack of knowledge rather than intent. To avoid falling in such a category, you first need to understand FCRA guidelines on disclosures and authorizations.

The essence of FCRA guidelines disclosures and authorizations is this: that no employee or applicant can have a background check carried out on them without their permission. Basically, although an employer has every right to carry out a background check, it is illegal to carry one out without getting authorization from the employee/applicant.

The FCRA provides a number of guidelines through which an employer can get permission from the employee or applicant. These guidelines are what make up the disclosures and authorizations.

They are summarized as follows:

- An employer must disclose to the employee or applicant that they intend to carry out a background check on them.
- The disclosure must inform the employee or applicant about the kind of information which may be unearthed during the background checks.
- The disclosure must be given in writing, and must be in "stand-alone" document i.e. it must not be part of any other document.
- An employer must secure a written authorization from the employee or applicant, permitting them to carry out the background check.
- An employer must inform the employee or applicant that they have a right to obtain a copy of the Consumer Report (i.e. the report which contains the information collected from the background check).

There are three aspects of the FCRA guidelines which may need a little elaboration:

The first is the concept of a "**stand alone disclosure.**" This basically means that any

the disclosure has to be given to the employee or applicant in a separate document. It shouldn't be embedded in any other document. The employee/applicant should be in position to easily identify the disclosure.

The reason for behind the "**stand alone**" nature is so that employers do not bury this information with the result that the applicant unintentionally authorizes a background check. This is why the disclosure is supposed to be separate from the employee/applicant's employment application.

In practice though, the disclosure and authorizations are often fused into a single document with two distinct parts. The first is a full disclosure detailing the intention to carry out the background checks. The second is the employee's/applicant's authorization (usually a declaration which they sign). The Federal Trade Commission (FTC) guidelines allow the disclosure and authorization to be in the same document.

The second is the right of the applicant/employee to obtain a copy of the background check. The FCRA guarantees this right. It offers them the right to request for a copy from the CRA (company carrying out the background check). As such, the disclosure is supposed to contain the name and contact details of the CRA.

The third is the timing of the disclosures and authorizations. The options are in relation to the request for a background check. The first (and most obvious) is before requesting a background check. Under this option, employers have to get disclosures or authorizations before requesting a background check.

In a nutshell, disclosure and authorization is among the easiest FCRA guidelines to comply with. It is also one of the easiest to violate. The consequences of violation – as

evidenced with the recent spate of FCRA class actions – can be quite severe. Therefore, every employer needs to make sure that they are in compliance.

The best part is that compliance is quite simple.

FCRA Compliance: Step 3 

Pre Adverse Action Notice

Sometimes, information unearthed during a background check can form the basis of taking what in FCRA lingo is referred to as an "**adverse employment action**". An adverse action is basically a decision which has negative implications for the employee/applicant. Examples include not hiring an applicant, firing an employee, demoting an employee or removing certain privileges.

If the background check was carried out by a CRA, then the FCRA has certain requirements which must be met before the adverse action can be carried out.

Among these requirements are the following:

- The employer must send a notice to the employee or applicant indicating their intention to carry out the adverse action. This notice is legally referred to as a "**Pre Adverse Action Notice**".
- The notice must include a copy of the Credit Report (background check report) on which the adverse action will be based.
- The notice must also include a copy of a document entitled "**A Summary of Your Rights Under the Fair Credit Reporting Act**." This document can be obtained

from the CRA which carried out the background check.

- The notice must include up-to-date contact information of the CRA (the company which carried out the background check).

Upon sending the Pre Adverse Action Notice, it is suggested that businesses give the employee or applicant up to a week to initiate a dispute. In case an applicant or employee doesn't dispute the information in the Report, the next step is to initiate the Notice of Adverse Action.

There are two important things which have to be observed when handling Pre Adverse Action Notices. The first is to ensure that you are using the latest and most up-to-date FCRA and CFPB forms. Failure to do so can lead to FCRA violations – with dire consequences.

A case in point is a recent class action lawsuit in which Kmart had to pay a $3 million settlement. The class action was brought about because Kmart failed to notify job applicants that they were rejected for failing a background check. The lawsuit was initially brought in 2011 after Kmart offered an applicant a job, but then withdrew it after carrying out a background check.

According to the suit, Kmart offered the applicant a copy of the background report together with an outdated statement of FCRA rights. The statement the applicant received was released in 1997 by the Federal Trade Commission (FTC). It contained inaccurate FTC and Federal Reserve contact information. It also didn't contain important revisions including the right for an applicant to dispute inaccurate or incomplete information.

Basically, sending a Pre Adverse Action Notice isn't enough. You have to ensure that all the information and forms sent along are accurate and up-to-date. Otherwise, you may end up in a situation like Kmart – having to pay a huge settlement even after trying your best to comply with FCRA guidelines.

The second important thing to note about a Pre Adverse Action Notice is giving an employee or applicant an opportunity to dispute.

The reason for this is that background checks aren't impeccable. Sometimes, they raise red flags which can easily be explained away. Therefore, it is required to allow employees or applicants an opportunity to explain themselves or dispute information in the report. This is highly advisable especially if they score highly in the attributes which you are looking for.

In a nutshell, before you take an adverse action as a result of information collected in a background check, FCRA regulations require you to send the applicant or employee a Pre Adverse Action Notice. Under normal circumstances, most CRAs can prepare and even send the notices on your behalf. Even then, you need you need to follow-up with them. Specifically, you need to ensure that any supporting documents they send are up-to-date and accurate.

FCRA Compliance: Step 4

Adverse Action Notification

Upon completing the **Pre Adverse Action process**, the EOCC also recommends

making an individualized assessment of before carrying out the adverse action. Basically, the adverse action should follow a process in which the employee or applicant has received a notification and had an opportunity submit a dispute.

If upon completing the process, you are still determined to carry out the adverse action, then you have to give the employee/applicant an Adverse Action Notification. This is simply a notification informing the employee/applicant that you have carried out an adverse action basing on information gathered in a background check.

The **Adverse Action Notification** can be given orally, in writing or electronically. There are certain pieces of information which should be contained in the notification.

Assuming that the adverse action was not hiring an applicant, the notification would include the following:

- A notice that he or she wasn't hired because of the information contained in the report.
- The name, address and telephone contact of the CRA (company which carried out the background check).
- Information which clarifies the fact that the CRA did not make the hiring decision, and cannot offer any explanation for the decision.
- Information about their right to dispute the accuracy or completeness of the background report and get an additional report from the CRA.

Employers who fail to provide to provide adequate notification to applicants or employees who face adverse action can suffer severe consequences. The FCRA allows employers who violate the terms of notifications to be sued for damages in

a federal court. Anyone who successfully sues is entitled to recover court costs and reasonable legal fees. The court can also award punitive damages for deliberate violations.

This provision makes adverse action lawsuits attractive to class action attorneys. The FCRA provides for recovery of statutory damages of between $100 and $1,000 per violation, as well as punitive damages and attorney fees. As such, adverse action lawsuits can be lucrative to attorneys. This fact has put numerous class action attorneys on the lookout – seeking for employers who violate adverse action provisions.

A single violation can open an employer up to a host of class action lawsuits. This is what happened in the recent class action against Delhaize America, LLC. One woman brought a suit against the company for a violation of FCRA disclosure requirements by its subsidiary, Food Lion, LLC. The smart attorneys went and gathered 57,000 people – anyone who had applied for employment at the Food Lion and been rejected – and brought a class action against the company their behalf.

However, the attorneys didn't stop there. They figured out that if Food Lion hadn't been making disclosures, chances are high that it hadn't been sending adverse

notifications as well. They were right. They soon gathered 2,500 people, anyone who had failed to get through Food Lion's interview process, and brought an adverse notification class action on their behalf.

In the end, Delhaize America, LLC had to agree to a settlement close to $3 million. The reputational damage that the company damage suffered was much worse. The plaintiffs didn't gain much from the settlement either. Each of the members in the disclosure class action received a paltry $31 while those in the adverse notification class action reviewed $61.

The real winners were the attorneys. They bagged one-third of the settlement fee – a cool $1 million. This is why attorneys love it when employers make FCRA violations! The employers lose big (their money and reputation goes), the applicants/employees win moderately (if you can term earning $61 after a year-long court battle as "winning"), but it is they – the attorneys – who win big.

Basically, if you an employer who still needs motivation for FCRA compliance, it is this: attorneys love it when you violate FCRA processes. To them, it is a huge payday. As such, they will pounce on the slightest violation and make a meal out of it. And, if the Delhaize America class action is anything to go by, as soon as you offer them a single opportunity through a small violation, they'll sniff around and discover more.

Unfortunately, class action attorneys aren't the only thing employers need to worry about. Another possible source of trouble is the Federal Trade Commission (FTC) or the Consumer Financial Protection Bureau (CFPB). The CFPB is charged with enforcing FCRA compliance. Unlike attorneys, the CFPB isn't motivated by a huge payday, but more concerned with consumer protection.

Over the last few years, the FTC has stepped up its crack down on employers who violate FCRA guidelines. The two most recent cases involve companies which failed to send pre-adverse action and adverse action notifications. In separate complaints, the FTC accused Quality Terminal Services LLC and Rail Terminal Services of failing to send pre-adverse and adverse action notifications. This occurred when the companies made hiring and firing decisions using information obtained through background checks.

To resolve the cases, the companies agreed to pay $24,000 and $53,000 in civil penalties. They also agreed to keep detailed records and periodically submit to FTC monitoring in order to ensure compliance with FCRA in the future.

The bottom line is that failure to comply with FCRA can have severe consequences for an employer. With smart attorneys and the FTC on the watch, an employer cannot be too careful. Fortunately, observing the FCRA regulations isn't that difficult. It may require some extra input from your staff, but it can be easily done. The last thing you want is to be slapped with a million dollar payout simply because someone on your staff forgot to send a letter.

FCRA Compliance: Step 5 05

Disposing of Background Information

Once you have no further use of the information gathered through background

checks, you may want to dispose of it. The legal guidelines which govern such a disposal are contained in Federal Trade Commission (FTC) regulations which are collectively referred to as "**the Disposal Rule.**"

The Disposal Rule governs the disposal of what it refers to as "consumer information." In the context of background checks, consumer information can mean two things. First of all, it refers to any reports or documents which contain the background information.

Secondly, it refers to any other information which is derived from the background reports, as long as the individual is identifiable. For instance, notes about a candidate made by a recruitment manager can be classified as "**consumer information**" – as long as there is sufficient information to identify the candidate.

The Disposal Rule provides guidelines on how such information should be disposed of. According to the Disposal rule, the term "disposal" can mean two things. The first is destruction of the information. The second is transfer of electronic equipment which contained the information (relevant for electronic information). We shall look at each of these in detail shortly.

In terms of destruction, the Disposal Rule does not stipulate specific methods by which background information should be destroyed. However, it states that whatever method is used should make it impossible to reconstruct the information in a manner which can be reused. It recommends methods such as shredding, burning or pulverizing for paper documents, and deleting, wiping or magnetically swiping for electronic records.

In terms of transferring electronic equipment (e.g. selling or donating computers which contain electronic copies of the information), the Disposal Rule recommends total destruction of the information prior to the transfer. The information should be irretrievable before the electronic equipment is transferred. Some recommended methods include deleting files, formatting the hard drive, or magnetically swiping the hard drive.

The Disposal Rule permits an employer to hire a disposal company to destroy the consumer information on its behalf.

Before hiring the company, the FTC advises the employer to perform due diligence which includes the following:

- review an audit of the disposal company's operations, including whether its operations comply with the Disposal Rule
- use information from several references to evaluate the disposal company
- require that the company possess certification from a reputable trade organization
- review and evaluate the company's policies or procedures, especially the ones regarding information security

It is important to note that the due diligence detailed above is not part of the Disposal Rule. As such, observing it isn't a must. However, it is a recommendation which is offered by the FTC to guide employers on how to vet disposal companies. Given the

sensitivity around consumer information, the due diligence can provide a rigorous framework through which an employer can select the perfect disposal company.

The Disposal Rule requires strict storage procedures to be observed before and during the destruction process. Under no circumstances should an unauthorized party be granted access to the consumer information – not even when it is on the verge of being destroyed.

The one aspect which the Rule doesn't explicitly spell out is how long the background information may be kept before destruction. It states that employers should consult the relevant federal and state laws which deal with storage of consumer information. This is because there are different laws and regulatory bodies which require information to be kept for various lengths of time.

The **EEOC** and the Department of Labor both have guideline for record retention.

However, setting time limits to keeping background records isn't limited to federal departments and regulatory bodies. Most state anti-discrimination statutes require employees to keep information regarding the hiring process for two years or more. In the event that a discrimination claim has been made, most states require that the relevant documents be kept until the case is closed.

There are also certain state laws which can influence how long background information is kept. For instance, in Oregon, employers are supposed to keep any records used to determine a person's suitability for hire, promotion and other personnel decisions for at least 60 days after termination of employment. If background information is among the records, then employers would be legally

bound to keep them for that time period.

The bottom line is that there are numerous laws and statutes whose provisions can influence how long you may store background information. It would have been easier if there was one law or statute. Unfortunately, the law can sometimes become very complex. Therefore, before you even make a decision to destroy background information, please check out the storage laws in your jurisdiction. Make sure that you are not breaking any law by destroying the information.

Once you have ascertained that it is perfectly legal to destroy the background information, then the Disposal Rule comes into play. The Disposal Rule provides every guideline you need in order to destroy the background information. In case you don't have the technical capacity to carry out a proper disposal, you can always hire a disposal company. Just remember to use the due diligence process which is recommended by the FTC.

With that, we come to the end of our Fair Credit Reporting Act (FCRA) compliance series. Hopefully, you now have a fair idea of the different FCRA provisions. So, the next time you intend to use background checks to inform your hiring decisions, please remember that there are legal guidelines which need to be followed.

Make sure you diligently follow the FCRA guidelines so that you don't join the infamous list of employers who violated the FCRA and ended up paying millions of

dollars in court settlements.

Crimcheck.com is a consumer reporting agency providing screening services since 1991. For more information go to, www.crimcheck.com or visit the FTC.

Disclaimer:

The materials available in this document are for general informational purposes only and not for the purpose of providing legal advice. These laws change frequently and varies from jurisdiction to jurisdiction. Being general in nature, the information and materials provided may not apply to any legal set of circumstances. You should contact your attorney to obtain advice with respect to any employment issue.