

Pamela Q. Devata is a labor and employment attorney in the Chicago office of Seyfarth Shaw LLP, where she specializes in Fair Credit Reporting Act and background screening compliance, counseling and litigation defense. She is active in Seyfarth's nationwide task force on the FCRA and is a former board member of the National Association of Professional Background Screeners (NAPBS). For more information about Seyfarth Shaw LLP, please visit www.seyfarth.com

It is no secret that identity theft has become a problem for consumers in recent years, costing millions of dollars in fraudulent purchases, credit fixes and litigation. As a result, the legislature and many government agencies including the Federal Trade Commission have taken measures to curb this rising trend. Indeed, recent regulations issued by the FTC and mandated by The Fair and Accurate Credit Transactions Act of 2003 (FACTA) have specific directives for users of consumer information that are aimed at uncovering and preventing incidents of identity theft. These new regulations go into effect on November 1, 2008 and require the creation of a number of new policies and procedures for specified entities. Some of the regulations apply to all users of consumer reports, where others are specific to financial institutions and creditors.

The Law

FACTA or the FACT Act as it is sometimes referred to went into effect in December 2003 and amended the federal Fair Credit Reporting Act (FCRA) in a number of ways. As it relates to identity theft prevention, FACTA instituted a procedure to help users of consumer reports combat identity theft by creating a notion of “red flags” when identity theft was suspected. In FACTA, a “Red Flag” is defined as a pattern, practice, or specific activity that indicates the possible existence of identity theft. A “user” of a consumer report includes entities such as employers who obtain consumer reports for the purpose of making employment (hiring, promotion, firing, etc.) decisions, as well as financial institutions, and granters of credit who use the information contained in consumer reports to issue credit cards, loans or mortgages, and other such activities.

FACTA's identity theft prevention sections require various federal agencies to implement regulations describing exactly what users must do to comply with the law. Two sections of the Act, 15 U.S.C. § 1681m (FACTA section 114), and 15 U.S.C. 1681c (FACTA section 315), refer specifically to the creation of such regulations. FACTA section 114, which addresses procedures users must implement in the case of an address discrepancy between themselves and a consumer reporting agency (CRA), applies to all users. FACTA section 315, which requires the implementation of an Identity Theft program pursuant to the Red Flags rule, is applicable only to financial institutions and creditors, as described below.

Because the law itself does not provide a lot of guidance on exactly what users need to do to be in compliance with the identity theft red flags, employers and other users should be aware of their responsibilities under these new regulations.

The Regulations

Address Discrepancies - Regulations For All Users of Consumer Reports

As of November 1, 2008, *all* users of consumer reports must adhere to the regulations regarding address discrepancies whenever they obtain consumer reports from a nationwide CRAs. Generally, nationwide consumer reporting agencies include Experian, Equifax, and Trans Union, but not other consumer reporting

agencies. These regulations apply to all employers, financial institutions and any other users of consumer reports. 16 CFR Section 681.1. The regulations detail specific requirements a user of consumer reports must follow when it receive notice of an address discrepancy from a nationwide CRA.

The term, “notice of address discrepancy” is a notice that informs the user that there is a “substantial difference” between the address it provided to the nationwide CRA when it requested the consumer report, and the address that the nationwide CRA itself has on file for that consumer or determines in creating the report. The term “substantial difference” has not been defined yet. It likely will not cover minor typographical difference between the two addresses, but any larger inconsistencies will likely require the sending of a notice to the user.

The next part of the regulation requires all users of consumer report information to implement reasonable policies to verify the identity of a consumer when a notice of address discrepancy is received. What does this mean? Basically, all users must implement procedures to deal with any notices of address discrepancy they receive from a nationwide CRA. These policies and procedures must be designed to help the user confirm that the consumer report and the consumer match, that is, that they both refer to the same individual, and that individual is the one for whom the user requested a consumer report in the first place. The regulations give examples of types of reasonable policies:

I. The user can have a policy to compare the information in the consumer report from the CRA with information the user:

- Obtains and uses to confirm the consumer’s identity pursuant to the requirements of the Customer Information Program (CIP) rules (31 U.S.C. 5318(1);
- Maintains in its own records, such as employment applications, change of address notices, or other customer account records; or
- Obtains from third-party sources. OR

II. It can have a policy to verify the information in the consumer report provided by the CRA with the consumer himself or herself.

The regulations also require the user to send a newly confirmed address back to the nationwide CRA. Section 681.1(d)(1) of the regulations mandates that users again develop reasonable procedures for informing the nationwide CRA that the user has confirmed a consumer’s address. The user, however, must only furnish the nationwide CRA with a confirmed address if the following criteria are met:

- The user can form a reasonable belief that the consumer report and the consumer do in fact refer to the same person, and that he or she is the person for whom the user requested a report in the first place;
- The user has a continuing relationship with the consumer; and
- The user regularly and in the course of business furnishes information to the CRA who provided the original notice of address discrepancy.

The regulations then provide examples of address confirmation methods users can employ:

- The user can verify the address with the consumer;
- The user can review its own records, such as employment applications or loan requests;
- The user can verify the address through third party sources; or
- It can use other reasonable means.

Finally, the regulations state that any policies and procedures implemented as a result of Section (d)(1) must have the user furnish a confirmed address to the nationwide CRA as part of the information it regularly furnishes for the reporting period in which it establishes a relationship with a consumer.

Because nationwide CRAs often resell consumer credit information to non-nationwide consumer reporting agencies who then make it available to employers and other users, it is unclear how, if at all, run of the mill consumer reporting agencies will be involved in the communication of the “notice of address discrepancy” and the user’s communication of a confirmed address. Potentially non-nationwide CRAs who are resellers of credit information may act as a conduit for the required notices – similar to their function when communicating consumer credit information. This remains to be seen.

Red Flag Regulations – Financial Institutions and Creditors Only

In addition to the general regulations that apply to all users of consumer reports, there are additional Red Flag regulations that apply specifically to financial institutions and creditors. These regulations are even more burdensome. Per the regulations, these entities must meet four basic requirements:

- Financial institution and creditors must periodically identify whether they maintain accounts covered by the regulations. Covered accounts are basically those involving or designed to allow, multiple payments or transactions. Examples include personal credit card accounts, residential mortgage loans, utility accounts, and other accounts for which there is a reasonably foreseeable risk of identity theft;
- Financial institution and creditors must establish an identity theft prevention program, as described below;
- The program must be administrated by the financial institution or creditor; and
- Each financial institution and creditor must consider the Red Flag guidelines set forth in Appendix A to the regulations and include in its identity theft prevention program those that are appropriate.

Identity Theft Prevention Program

As explained above, one part of the regulations requires the establishment of an identity theft prevention program that is designed to “detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account.” Such program must include reasonable policies to:

- Identify relevant Red Flags for the covered accounts that the financial institution or creditor offers, and incorporate those Red Flags into its Program;
- Detect Red Flags that have been incorporated into the Program;
- Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft; and
- Ensure that the Program is updated periodically.

Conclusion Any and all users of consumer report information should be aware that the new identity theft regulations go into effect on November 1, 2008 and may require covered entities to implement a number of carefully considered policies and procedures. Employers and other entities covered by the regulations should consult with an experienced labor and employment attorney before implementing any sort of identity theft prevention program.