AN ALERT FROM THE BDO NONPROFIT SERVICES PRACTICE

BDO KNOWS:
NONPROFIT SERVICES

▶SUBJECT

THE RED FLAGS RULE – WHAT DOES IT MEAN TO NONPROFIT ORGANIZATIONS?

▶DETAILS

One of the largest growing areas of criminal activities in the past decade has been identity theft. Identity theft occurs when an individual uses other people's personally identifying information to assume their identity, open new accounts as well as misuse existing accounts. In doing so, they are creating havoc for consumers and businesses and all other parties involved.

The Federal Trade Commission (FTC), the Federal bank regulatory agencies, and the National Credit Union Administration (NCUA) have issued regulations entitled the Red Flags Rule requiring financial institutions and creditors to develop and implement written identity theft prevention programs as part of the Fair and Accurate Credit Transactions (FACT) Act of 2003. FACT adds several new provisions to the Fair Credit Reporting Act of 1970.

The FTC has extended the effective date of the regulation until December 31, 2010, to give creditors and financial institutions additional time in which to develop and implement written identity theft prevention programs. This deferral by the FTC does not affect other federal agencies' enforcement of the original November 1, 2008, deadline for institutions subject to their oversight to be in compliance. Under the Red Flags Rule, any instance of identity theft exposes the NFP organization to an FTC investigation and potential fines.

▶Read more

THE "RED FLAG PROGRAM CLARIFICATION ACT OF 2010"—which generally exempts lawyers, accountants, health care and other service providers from being classified as "creditors" for the purposes of the Fair Credit Reporting Act (FCRA), as amended by the Fair and Accurate Credit Transactions Act of 2003—was signed into law by President Obama on December 18, 2010. The legislation stipulates, in part, that the term "creditor" refers only to a business "that regularly and in the ordinary course of business (i) obtains or uses consumer reports, directly or indirectly, in connection with a credit transaction; (ii) furnishes information to consumer reporting agencies, as described in section 623 of FCRA, in connection with a credit transaction; or (iii) advances funds to or on behalf of a person, based on an obligation of the person to repay the funds or repayable from specific property pledged by or on behalf of the person." The law also clarifies that the third item does not include funds advanced on behalf of a person "for expenses incidental to a service provided by the creditor to that person." Organizations will need to seek legal advice to determine if the activities of their organization are affected by this new legislation.

CONTACT: LEE KLUMPP
Director, Assurance Services
lklumpp@bdo.com /301-634-4921

WHO MUST COMPLY WITH THE RED FLAGS RULE?

In the regulations, the Red Flags Rule (the Rule) is applied to "financial institutions" and "creditors" with "covered accounts."

Under the Rule, a *financial institution* is defined as a state or national bank, a state or federal savings and loan association, a mutual savings bank, a state or federal credit union, or any other entity that holds a "transaction account" belonging to a consumer. Most of these institutions are regulated by the Federal bank regulatory agencies and the NCUA. Financial institutions under the FTC's jurisdiction include state-chartered credit unions and certain other entities that hold consumer transaction accounts.

A *transaction account* is a deposit or other account from which the owner makes payments or transfers. Transaction accounts include checking accounts, negotiable order of withdrawal accounts, savings deposits subject to automatic transfers, and share draft accounts.

A *creditor* is any entity that regularly extends, renews, or continues credit; any entity that regularly arranges for the extension, renewal, or continuation of credit; or any assignee of an original creditor who is involved in the decision to extend, renew, or continue credit. Accepting credit cards as a form of payment does not in and of itself make an entity a creditor. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. Where nonprofit and government entities defer payment for goods or services, they too are to be considered creditors. Most creditors, except for those regulated by the Federal bank regulatory agencies and the NCUA, come under the jurisdiction of the FTC.

A *covered account* is an account used mostly for personal, family, or household purposes, and that involves multiple payments or transactions. A covered account is also an account for which there is a foreseeable risk of identity theft.

WHAT DOES THE RED FLAGS RULE REQUIRE?

The Red Flags Rule requires that financial institutions and creditors (as defined above) implement a plan to identify, detect and respond to attempts to use stolen identity information. The FTC did not specifically state what the indicators of potential identity theft may be. The regulations require each organization to perform a risk-assessment of their day-to-day operations and identify where and how someone could perpetrate a theft of someone else's identity to steal from the organization.

The organization's program must state who is responsible for implementing and administering it effectively. Because employees have a role to play in preventing and detecting identity theft, the program also must include appropriate staff training. The program also must address the manner in which contractors will be monitored when the organization outsources or subcontracts functions or operations that would be covered by the Red Flags Rule.

Some examples of activities that would subject an organization to the Red Flags Rule follow:

- Colleges, universities and schools that allow for tuition to be paid in installments for the school semester or year.
- Debt collectors, loan processors, and others who handle credit accounts.
- Hospitals and clinics that do not require full payment at discharge and bill for services.
- Charities that take multiple payment pledges in which donors provide personal information such as a bank account and/or credit card information and the nonprofit processes the payments.
- Professional service providers such as doctors, dentists and other healthcare providers that bill after the services have been delivered.
- Retail operations of a nonprofit that allow payment plans or issue private credit cards.
- Trade associations, clubs and other non-profit organizations that allow members or donors to pay dues or pledges in installments.

▶Read more

The National Association of College and University Business Officers (NACUBO) has identified several areas "that could cause colleges and universities to be considered 'creditors' under the Rule, including participating in the U.S. Department of Education Student Loan Program or state loan programs; offering institutional loans to students, faculty, or staff; and/or offering a plan for payment of tuition throughout the semester or year rather than requiring full payment of tuition at the beginning of the semester".

Additionally, several other nonprofits that represent various types of organizations have gone on the record as stating that the Red Flags Rule could apply to organizations that use consumer credit reports when they conduct credit or background checks on prospective employees or applicants. The Red Flags Rule was written by the FTC to ensure that virtually any type of organization that does not require full payment up front will fall under the regulations. Therefore, if your nonprofit organization sends invoices, your organization is probably covered by this rule.

The Red Flags Rule envisions that the nonprofit organizations will identify potential identity theft through the use of red flags.

A red flag might be someone who is presenting suspicious identification in order to obtain some type of credit or deferred payment, multiple address changes in a short period of time, or a notification from a credit reporting agency that there is an issue with an individual's credit history. The Rule requires you to identify all of the indicators that might tip you off to possible identity theft, implement appropriate predictive and detective controls, and react appropriately.

COMPLYING WITH THE RED FLAGS RULE

The Red Flags Rule requires many nonprofit organizations to implement a written Identity Theft Prevention Program that is designed to detect the warning signs ("red flags") of identity theft in their nonprofit organization's day-to-day operations.

These may include, for example, unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. The program must also describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program. The program must be managed by the Board of Directors and/or senior employees, include appropriate staff training, and provide for oversight of any service providers.

The following are four suggested steps in developing an identity theft program for your organization to comply with the Red Flags Rule:

1) Identify the red flags associated with identity theft that are likely to be seen by your nonprofit organization. The program must include reasonable policies and procedures to identify the "red flags" of identity theft that may arise in the day-to-day operation of your business. Red flags are suspicious patterns or practices or specific activities that indicate the possibility of identity theft. For example, if a customer has to provide some form of identification to open an account with an entity, an ID that looks like it might be fictitious would be a "red flag."

2) Set up procedures to detect those red flags in your nonprofit organization's day-to-day operations. The program must be designed to detect the red flags that have been identified. For example, if an entity has identified fake IDs as a red flag, it must have procedures in place to detect possible fake, forged, or altered identification.

3) If your staff or you spot any red flags that you have identified, you need to make sure that your organization responds appropriately to prevent and mitigate the harm done. The program must spell out appropriate actions to take when red flags are detected.

▶Read more

4) Just like any other set of policies and procedures that your nonprofit organization designs and implements, the red flag policies and procedures need to be reevaluated from time to time. This is especially true in this instance since risks of identity theft can change rapidly, so it's important to keep your nonprofit organization's policies and procedures current related to red flags. Additionally, the education of your staff will need to be an ongoing process. This is because the education process needs to continue on an ongoing basis to continually update your employees as the risk of identity theft changes. The program must address how you plan to reevaluate the program periodically to incorporate and address new risks from this crime because identity theft is an ever-changing threat.

The Red Flags Rule provides all affected entities with the opportunity to design and implement a program that is appropriate to their size and complexity, as well as the nature of their operations. Guidelines issued by the FTC, the Federal banking agencies, and the NCUA that may be found at http://www.ftc.gov/opa/2007/10/redflag.shtm should be helpful in assisting covered entities design their programs. A supplement to the guidelines identifies 26 possible red flags. These red flags are not a checklist, but rather are examples that affected entities may want to use as a starting point. They fall into five categories:

- Alerts, notifications, or warnings from a consumer reporting agency;
- Suspicious documents;
- Suspicious personally identifying information, such as a suspicious address;
- Unusual use of or suspicious activity relating to a covered account; and
- Notices from customers, victims of identity theft, law enforcement authorities, or other businesses about possible identity theft in connection with covered accounts.

▶RESOURCES

The Federal Trade Commission has issued several publications that outline what an organization needs to do related to the Red Flags Rule and things that should be considered. The publications listed below can be found on the Federal Trade Commission's web site and offer additional resources:

New "Red Flag" Requirements for Financial Institutions and Creditors Will Help Fight Identity Theft at http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

The "Red Flags" Rule: Are You Complying with New Requirements for Fighting Identity Theft? at http://www.ftc.gov/bcp/edu/pubs/articles/art10.shtm

Fighting Fraud with the Red Flags Rule: A How-To Guide for Business at http://www.ftc.gov/redflagsrule

The Red Flags Rule at http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf