COUNTY ADVISORY BULLETIN

CAB

Published by: County Commissioners Association of Ohio

37 West Broad Street, Suite 650 • Columbus, Ohio 43215-4195
Phone: 614-221-5627 • Fax: 614-221-6986 • www.ccao.org

Bulletin 2008-01 **October 2008**

FEDERAL REGULATIONS REQUIRE SOME COUNTIES TO DEVELOP "RED FLAG" IDENTITY THEFT PROGRAMS

Public Law 108–159

LEGISLATIVE HISTORY—H.R. 2622 (S. 1753):

CONGRESSIONAL RECORD, Vol. 149 (2003):
Sept. 10, considered and passed House.
Nov. 5, considered and passed Senate, amended, in lieu of S. 1753.
Nov. 21, House agreed to conference report.
Nov. 22, Senate agreed to conference report.

WEEKLY COMPILATION OF PRESIDENTIAL DOCUMENTS, Vol. 39 (2003):
Dec. 4, 2003 Presidential remarks.
15 USC 1681m.

Effective Date: Written programs must be in place by November 1, 2008*
(*Enforcement will be suspended until May 1, 2009.)

Bill Summary

In response to growing concerns over increasing identity theft, the federal government recently passed a law requiring various federal agencies to develop and enforce guidelines that, in turn, require local governments, as well as financial institutions and creditors, to develop and implement written identity theft programs.

The regulations the Federal Trade Commission and other federal agencies developed have become known as the "Red Flags Rules." The Red Flags Rules require each local government, financial institution, or creditor that holds any consumer account, or other account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program.

Sections of Bulletin

1. What is a "Red Flag"?
2. Do the Red Flags Rules affect my county?
3. Specifically, what county programs are covered by the red flag rules?
4. When does enforcement begin?
5. What are the penalties or liability for non-compliance?
6. What elements must my Program include?
7. How do I administer the Program?
8. Is there a sample program available?
9. How long should it take to write the Program?
10. Where can I get more information on the Red Flags Rules?

1. What is a "Red Flag"?

Simply put, a red flag is a warning sign. Specifically, a red flag in the context of the FTC's "Red Flags Rules" is a warning sign that a person's identity has been stolen for purposes of economic fraud.

2. Do the Red Flags Rules affect my county?

The Red Flags Rules apply to "financial institutions" and "creditors" with "covered accounts."

The Federal Trade Commission, which is in charge of writing administrative rules, opines that 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. Creditors include finance companies, automobile dealers, mortgage brokers, utility companies, and telecommunications companies. ***Where non-profit and government entities defer payment for goods or services, they, too, are considered creditors.***

Thus, if a county (or group of counties) entity (Entity) provides a program that extends a good or service for which payment is deferred, that program is indeed subject to the FTC rules.

3. Specifically, what county programs are covered by the red flag rules?

In conversations with the Federal Trade Commission, it appears that if a county operates a county water and sewer system that the red flag rules would apply. This is because service is provided prior to the time a bill for water and sewer service is rendered to the customer. On the other hand, we believe that the red flag rules would not apply to the payment for a dog license because there is a specific payment due date, and no service is being rendered for the license.

Whether other county programs and functions are covered by the red flag rules is not well defined. In working with other state associations on this issue, North Carolina, for example, told counties in that state:

"**Counties may also have to administer a Program if the county establishes customer accounts that are designed to permit multiple payments or transactions for non-utility services or products that are consumed or used primarily for personal, family, or household purposes, and for which payment is deferred into the future.** It is unclear to what types of non-utility accounts the rules apply, but it appears that some services in the health

and human services arena, such as emergency medical transport, public health clinics, and disabled transport services, may trigger the Red Flag Rules."

In this regard, we like North Carolina, suggest that this be discussed with the County Prosecutor.

4. When does enforcement begin?

On October 22, the Federal Trade Commission (FTC) announced that enforcement of the Red Flag Rules will be suspended until May 1, 2009. The action was taken to give entities more time to develop and implement a written identity theft prevention program. The FTC acknowledged that many entities were not aware they were subject to the Rule and had learned of the requirements too late to come into compliance by the original November 1, 2008 deadline.

5. What are the penalties or liability for non-compliance?

Under the Federal Trade Commission Act (15 U.S.C. §§41 et seq.) the FTC may, in the event of a knowing violation, commence a civil action of up to $2,500 per violation. In determining the amount of this civil penalty a court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and other such matters as justice may require.

6. What elements must my Program include?

The FTC rules require that each entity that offers or maintains one or more covered accounts must develop and implement a written Identity Theft Prevention Program (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.

However, it is important to note that the rules specifically call for the program to be appropriate to the size and complexity of the financial institution or creditor and the nature and scope of its activities.

The Program must include reasonable policies and procedures to do all of the following:

> (i) Identify relevant Red Flags for the covered accounts that the entity offers or maintains, and incorporate those Red Flags into its Program;
>
> (ii) Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft;
>
> (iii) Ensure the Program (including the Red Flags applicable) is updated periodically to reflect changes in risks to customers

7. How do I administer the Program?

Each entity that is required to implement a Program must provide for the continued administration of the Program and must do all of the following:

(1) Obtain approval of the initial written Program from either its board of directors or an appropriate committee of the board of directors *(for example, a board of county commissioners, or in the case of a joint district entity, the board of directors);*

(2) Involve the board of directors, an appropriate committee thereof, or a designated employee at the level of senior management *(such as an executive director)* in the oversight, development, implementation, and administration of the Program;

(3) Train staff, as necessary, to effectively implement the Program (*put program in your training manuals*);

(4) Exercise appropriate and effective oversight of service provider arrangements if applicable *(for example, an entity may use a 3rd party billing operation).*

In addition staff should report, at least annually, to the board of directors or a designated employee at the level of senior management on the entity's compliance with the Red Flags Rules. The report should address the following: (1)The effectiveness of the entity's policies and procedures in addressing the risk of identity theft; (2) service provider arrangements; (3) significant incidents involving identity theft and management's response; and (4) any recommendations for changes to the Program.

8. How long should it take to write the Program?

As mentioned earlier, the rules specifically call for the program to be appropriate to the size and complexity of the entity and the nature and scope of its activities. To the extent that entities determine that they have a minimal risk of identity theft, the FTC staff believes that the time it would take to develop a program, train employees, and draft an annual report on risks of identity theft that are minimal or non-existent would be approximately 1 hour.

(*After preliminary discussions with FTC staff, most local government programs would likely fall under a minimal risk level, however each program is unique and may present unique and potentially higher levels of risk.)*

9. Is there a sample program available?

CCAO has drafted a sample program (attached) for counties to use for their various entities that offer services that would be subject to the red flag rules. Please not this is only a sample program and may need to be refined given the particularities of your own entity.

10. Where can I get more information on the Red Flags Rules?

The Federal Trade Commission (FTC) was the federal government agency that promulgated the rules that affect local governments as part of the federal Fair and Accurate Credit Transactions (FACT) Act of 2003. The FTC's website address is www.ftc.gov. For FTC inquiries, please call: (202) 326-2222.

As always, please don't hesitate to contact CCAO policy staff regarding questions on CABs. CCAO Policy Analyst Josh Hahn primarily authored this advisory bulleting. You can reach Josh at 614-221-5627 or jhahn@ccao.org.

--sample—

Long County Water & Sewer District Identity Theft Program

In response to the Federal Trade Commission Red Flags Rules, the Long County Water & Sewer District hereby adopts this identity theft program.

Administration:

- (Example: Director Smith) (LCWSD governing body, an appropriate committee of the governing body or a designated employee at the level of senior management) shall be responsible for the development, implementation, oversight and continued administration of the Program.

- The Program shall train staff, as necessary, to effectively implement the Program; and

- The Program shall exercise appropriate and effective oversight of service provider arrangements.

- (Director Smith) will present a report to the Long County Commissioners at least annually. The report will highlight all of the following:

    (1) Effectiveness of the entity's policies and procedures in addressing the risk of identity theft;
    (2) service provider arrangements;
    (3) significant incidents involving identity theft and management's response; and
    (4) any recommendations for changes to the Program.

The Program:

The LCWSD is ensured with various sensitive customer account information in providing the various services offered by the District. As part of ensuring the proper response to potential identity theft, all employees are charged with forwarding any of the following incidents that may raise a "red flag" as to identity theft to their immediate supervisor or Director Smith:

Suspicious Documents, such as

- An application or document provided for identification appears to have been altered or forged.

- The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

- Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

Suspicious Personal Identifying Information, such as

- Personal identifying information the customer provides is not consistent with other personal identifying information provided by the customer or with existing information on file. (*For example, there is a lack of correlation between the SSN given and the SSN already on file).*

- Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party source.

- The SSN, address, or telephone number provided is the same as that submitted by other persons opening an account or other customers.

- The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

- Shortly following the notice of a change of address for a covered account, the entity receives a request for the addition of authorized users on the account.

- A customer uses a covered account that has been inactive for a reasonably lengthy period of time (taking into consideration the type of account, the expected pattern of usage, and other relevant factors).

- Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's account.

- The entity is notified that the customer is not receiving paper account statements or of unauthorized changes or transactions in connection with a customer's covered account.

Mitigation of Identity Theft Following Red Flag Incident:

(Director Smith) in his capacity as Director of the LCWSD Identity Theft Program shall take any of the following actions he deems appropriate in response to a suspected threat of identity theft.

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing any passwords, security codes, or other security devices that permit access to a covered account;
- Not opening a new covered account;
- Closing an existing covered account;
- Notifying law enforcement *(county sheriff or county prosecutor)*;
- Determining that no response is warranted under the particular circumstances.

Updating the Program:

The Program shall be updated periodically to reflect changes in risks to customers or to the safety and soundness of the organization from identity theft based on factors such as:

1. Experiences of the organization with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the organization offers or maintains;
5. Changes in the business arrangements of the organization, including mergers, acquisitions, alliances, joint ventures, and service provider arrangements.