

HOT TOPIC – RED FLAG RULES
IGFOA CHICAGO METRO CHAPTER LUNCHEON
OCTOBER 3, 2008

1. Federal Identity Theft Prevention Requirements.
2. Fair and Accurate Credit Transactions “FACT” Act passed in December 2003 added provisions to the Fair Credit Reporting Act.
3. Regulations and guidelines for **Detection, Prevention and Mitigation of Identity Theft**.
4. **“Red Flag”** means a pattern, practice or specific activity that indicates the possible existence of identity theft.
5. Who do these rules apply to? Financial institutions and creditors that have “covered” accounts.
6. **Covered Account** – For our purposes means any account that permits multiple payments or transactions such as a utility account.
7. **Compliance with Red Flag Rules must be done by November 1, 2008.**
8. Compliance is through a written program of “reasonable” policies and procedures.
9. First step is a risk assessment
 - a. Determine whether you have covered accounts
 - b. If so, consider
 - i. Methods used to open accounts
 - ii. Methods access is provided to account information
 - iii. Any previous experience with identity theft
10. **Rules are designed to be flexible.** Design and implementation of the program that is appropriate to the size, complexity and nature of the operations.
11. Next step, elements of a written plan include:
 - a. Identify **relevant** red flags (internal and external).
 - i. Five categories with 26 examples, Supplement A to Appendix A.
 1. Alerts, Notifications or Warnings.
 2. Suspicious Documents.
 3. Suspicious Personal Identification Information.
 4. Unusual Use or Activity on an account.
 5. Notices of Possible Identity Theft by customers, others.

- b. Detect Red Flags – once identified, training of front-line staff to detect red flags.
- c. Appropriate response to any Red Flags detected – supervisor notified, response set forth in written policy.
 - i. Responses range from monitoring account, contacting the customer or changing passwords to determining no response is warranted.
- d. Provisions for ongoing administration of the plan – annual/periodic updates. Obtain approval of initial written program from governing authorities. Designate staff person in the oversight, development, implementation and administration of the program.

12. Penalties for non-compliance

- a. Federal Court Penalties of up to \$2,500 per violation
 - i. Per day for non compliance
 - ii. Per incident of identity theft if no formal program is in place
- b. Also be subject to State action
- c. Civil litigation for losses as a result of identity theft

13. Sources are available

- a. FTC website
- b. IML/IGFOA articles
- c. Other professional associations (IMUA)
- d. Colleagues – Jodie, Mark
- e. IGFOA website

For Seminar – Notes from Ed McKee, Village of Winnetka Finance Director

My comments are based on a seminar the Illinois Municipal Utilities Association sponsored last month in Springfield. I have shared some of this information with Maryanne and it is available on the IGFOA website, in the resource center database under the utility billing tab.

1) **What we do now to establish a utility account**

In Person - Card w/ information

Phone – take information and mail card

Service address, phone number, start date, if renter, deposit amount

* Ask Audience does anyone collect more information than this, is it verified?

2) **What we believe is required.**

The Village believes that the Fair Credit Reporting Act and Fair Credit Transactions Act of 2003 (public law 108-159) requires more information than we currently collect.

Effective 11/1/2008 must establish a written program approved by your governing board to **prevent, detect, and mitigate** the impact of **identity theft**.

You must have a reasonable belief the person requesting service is the person they represent themselves as (and retain that evidence).

Part of the detection is to establish red flags, circumstances that indicate there **COULD BE** an identity theft issue. The IMUA sample suggests 26 red flags might be applicable. Winnetka has narrowed that list to 13 we believe are required to meet the intent of the law.

I suggest that when you establish your red flags that you be as logical as possible. For example, if you choose to, you can accept personal knowledge of the applicant as acceptable ID verification. How you would document accepting personal knowledge as ID and avoid potential claims of different treatment for different customers is less clear.

Also not clear is the question of accepting information provided by a potential customer that appears to be genuine without confirming it with a third party. I think accepting what appears to be a valid driver's license from someone in person establishing an account is sufficient.

If someone is signing up over the phone and gives you the last four numbers of their social security number, I am not sure that is sufficient information unless that data is confirmed. Some communities use an identity checking firm to verify that the information collected is valid.

Some communities currently go so far as to collect social security numbers, previous service address, and other data that I would prefer to avoid because collecting that data increases the odds that a customer will believe, rightly or wrongly, that the Village's mishandling of an account lead to their identity theft.

We also have to train our staff on how to spot the red flags. Another way of thinking about red flags is that they are a pattern, practice, or activity that indicates identity theft might be present.

We also have to report on the policy annually to the governing board under the law.

3) Winnetka is taking the following steps

The Village has drafted an identity theft program based on the sample provided by the Illinois Municipal Utilities Association.

The Village selected 13 red flags as most relevant (26 are identified in the legislation) for our use.

We are working out the operational complexity of how to administer on a day to day basis the new requirements. This material will be sent to the Village Attorney and will be discussed with our Village Council in about a week. I think it is likely that the Village will adopt an identity theft prevention policy in two weeks.

I want our Council to be aware of 1) this law, 2) the policies we are proposing, and 3) the consequences of those policies.

Going forward, my hope is that:

- 1) My hope is that Municipalities consider adopting similar programs to prevent, detect, and mitigate the impact of identity theft, including the

selection of red flags that are most applicable. I think it is helpful to keep the policies and procedures as simple as possible to enhance compliance and make training easier.

- 2) My hope is that Municipalities consider similar steps to establishing and accessing accounts. For example, I think it will be problematic initially to explain to customers in your town why they need to verify identity before discussing account details over the phone when a neighboring community does not. I think most of us now routinely discuss account information with customers without making any effort to confirm identity. I think that is a problem under the new law.
- 3) My hope is that IGFOA and others offer additional assistance to us to meet the requirements of the law. I believe the steps we are taking now may very well be revised or adjusted over the next few years. I think what we are doing now shows a good faith effort at compliance and I hope our Village Attorney agrees with our opinion of that.

I could talk for quite some time about the operational problems related to the day to day requirements, but suffice it to say that each town has to work out something that is reasonable for you and that your Attorney feels is sufficient to meet the new legal requirements.

I thank you for your interest in this topic. The IGFOA is a good resource and there is some information out there that you can take and modify to meet your needs.

I will also say that this was somewhat of a sleeper bill in that it really didn't catch my attention early enough and the depth of its impact on our operations did not resonate with me until the last few weeks or so.

I will be around after the seminar for questions