

The Fair and Accurate Credit Transactions (FACT) Act of 2003 was created to prevent identity theft at financial institutions or other creditors, including utility companies. Identity theft is a fraud attempted or committed using identifying information of another person without authority and it results in billions of dollars in losses each year to individuals and businesses, according to a report of the President's Identity Theft Task Force. The Act requires that companies create a comprehensive "Identity Theft Prevention Program" to identify, detect, and respond to potential identity theft. The programs must be in place by November 1, 2008.<sup>1</sup>

The FACT Act requires utility companies to develop a written program that identifies and detects the relevant warning signs — or "red flags" — of identity theft. These may include, 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 resolve the crime and detail a plan to update the program regularly. The program must be appropriate to the organization's size and complexity and managed by the Board of Directors or senior employees. Additionally, it must include necessary staff training and provide for oversight of any third party service providers.<sup>2</sup>

There are many resources available to utility companies to create an identity theft prevention program. See the steps and online links below for an outline of the steps to create a Red Flag Program.

### **1. Review the regulatory specifics in the Federal Register**

See the FACT Act of 2003:

<http://frwebgate5.access.gpo.gov/cgi-bin/PDFgate.cgi?WAISdocID=839061302751+42+1+0&WAISaction=retrieve>

Read the Federal Trade Commission Business alert here:

<http://www.ftc.gov/opa/2007/10/redflag.shtm>

### **2. Determine applicability to the accounts you maintain and offer**

See appendix J to part 334, (page 46 of the federal register document above) for examples of covered accounts, this list is not to be used as a "checklist" to automatically include in your program, but a starting place of potential accounts.

### **3. Conduct an assessment to determine exactly where and how you maintain personal identifying information**

Developing this program can be an opportunity to streamline the processes and procedures in dealing with customer information. You can use this time to carefully look at how personal information is handled.

---

<sup>1</sup> <http://www.ftc.gov/opa/2007/10/redflag.shtm>

<sup>2</sup> <http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm>

#### **4. Develop and conduct a risk assessment**

See this document for more detailed steps, along with examples of potential red flags  
[http://info.ethicspoint.com/files/web\\_seminars/2008/Red\\_Flag/Red\\_Flag\\_Risk\\_Assessment.pdf](http://info.ethicspoint.com/files/web_seminars/2008/Red_Flag/Red_Flag_Risk_Assessment.pdf)

Engage any potentially affected departments, from customer service to legal, as a complete risk assessment will be the cornerstone of an effective program.

#### **5. Perform an industry benchmark evaluation**

Where is the company at now? What is working, what is not?

#### **6. Evaluate any existing identity theft prevention and anti-fraud programs**

The steps to identify and prevent identity theft may already be in place. Evaluate and record the procedures already in place, you may already be doing all you need to do. In this case, to satisfy the requirements, you simply need to create a new document, and have it approved by your board of directors.

#### **7. Assess the red flags you employ for appropriate risk levels and currency**

Are the existing programs effective in recognizing and addressing potential identity theft?

#### **8. Evaluate your red flag monitoring systems and methodologies**

How will you monitor, resolve and document red flag occurrences? If you work with third party providers, consider how there will be effective oversight of customer information with them as well.

#### **9. Evaluate the training program you have for key 'relevant' personnel**

To effectively implement the program, personnel must be trained to recognize and respond to Red Flags appropriately.

#### **10. Contact your regulator to discuss what they will be expecting on November 1, 2008.**

#### **11. Compose your written Identity Theft Prevention program**

It must outline how your company will:

1. Identify relevant Red Flags for the covered accounts that your company offers or maintains, and incorporate those Red Flags into the Program.
2. Detect Red Flags that have been incorporated into the program.
3. Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft.

4. Ensure the Program is updated periodically, to reflect changes in risks to customers and to the safety and soundness of stored information.

**12. Obtain and document approval of the written program from either your Board of Directors or an appropriate committee of the board of directors**

**13. Train staff, as necessary, to effectively implement the program**

**14. Review the program regularly to modify and add red flags, as well as update your company's Red Flag identification, detection and response.<sup>3</sup>**

The Kentucky Municipal Utilities Association is comprised of the Municipal Electric Power Association of Kentucky and the Municipal Water and Waste Water Association of Kentucky. KMUA members provide the essential services of water, waste water, electricity, natural gas and broadband. We take pride in providing low-cost, efficient and reliable service to almost a million citizens in cities throughout the Commonwealth of Kentucky. KMUA represents locally owned and operated utilities that are governed by city officials or independent utility boards appointed by city officials.

---

<sup>3</sup> <http://info.ethicspoint.com/newsandevents/event08150801.asp#supportmaterial>