ety in size of the airports involved in the pilot, Beckman says that no timetable has been set on when a standard biometric framework should be in place at the participating locations.

"We're moving forward and creating the paths to get there. I think you will see the bigger airports online sooner than a small airport that maybe doesn't have the resources to get to that point," Beckman says.

Though the TSA declined to discuss any details related to the BASIC program, the agency did say in a statement that it "encourages" airports to be proactive in implementing biometric access control and credentialing systems.

Government Mandates

Despite the advancements being made in credentialing security through BASIC, Richard Duncan, CPP, aviation security director for Hartsfield-Jackson International Airport in Atlanta, believes that government mandates may be required for many airports to jump on board

> "We have representatives on the BASIC working group, but it will still require some type of proposed rule making (by the government) before it can be implemented at the airports because of the costs associated with securing the materials for that program."
>
> **– Richard Duncan, aviation security director, Hartsfield-Jackson Intl. Airport**

Compliance Scorecard

Security Leadership Solutions Executive Council

Is Your Business Subject to the Red Flags Rule?

By Marleah Blades

In November 2007, the FTC and other agencies issued the Final Rule on Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003, more commonly known as the Red Flags Rule. This set of regulations requires financial institutions and creditors to develop, implement and regularly update a written identity theft prevention program that will recognize indicators (red flags) of possible identity theft attempts in connection with covered accounts and work to prevent and mitigate the risk of such attacks.

The rules set an initial compliance deadline of November 2007, but the FTC granted two subsequent extensions to allow businesses to better prepare for enforcement, re-setting the final deadline to August 1, 2009. The U.S. Code authorizes the FTC to levy civil penalties of up to $2,500 per violation.

Many businesses have complained that the rules define "creditor" too loosely, creating an undue burden on small businesses that don't see themselves as likely targets for identity theft. The rules define "creditor" as "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."

While the rule notes that accepting credit cards does not make an entity a creditor, the FTC's literature on the rules is equally clear that "creditor" is a broad category. It includes businesses, non-profits and government entities that regularly defer payment for goods or services, as well as those that provide goods or services and then bill customers later. Several types of non-financial entities may fall under this category, such as automobile dealers, mortgage brokers, utility companies, telecommunications companies, lawn care companies, house cleaning businesses, lawyers, franchisors and health care providers.

Clearly, many businesses that may not have the FTC, identity theft or regulation on their radar could be subject to the Red Flags Rule. It's a good idea to assess your business practices and check out FTC resources to determine if you fall into this category.

The FTC has published a number of resources to assist businesses large and small with compliance. Most of these are linked from their new Red Flags homepage: http://www2.ftc.gov/redflagsrule. From this site, you can also download a Red Flags How-To Guide for businesses that includes extended definitions of terms and requirements, answers to frequently asked questions, and a four-step process for compliance.

Marleah Blades is senior editor for the Security Executive Council (SEC). The Security Executive Council maintains a large and growing list of laws, regulations, standards and guidelines that impact security (https://www.securityexecutivecouncil.com/public/lrvc). Help the Council fill out the list and receive a selected complimentary metric slide from our store.