

CREDIT UNION TIMES

[Advertise](#) | [Contact Us](#)

HOME

SECTIONS

CLASSIFIEDS

PODCASTS

DIRECTORY

CALENDAR

SUBSCRIPTIONS

Welcome!


[Log into Credit Union Times](#)

Search Credit Union Times



ENROLL NOW, AND START
TEMPTING NEW MEMBERS
RIGHT AWAY.

**Credit
Union 24**
It's Your Network.

CLICK HERE

Red Flags Hover as November Nears

May 07, 2008

[E-Mail this article](#) | [Print this article](#)
By [Marc Rapport](#)

SAN DIEGO — Seems like it was just yesterday when credit unions were scrambling to meet the new FFIEC requirements for protecting consumer identities online.

Now the talk has turned to Red Flag. It's a sweeping collection of regulations ordered up by Congress in the Fair and Accurate Credit Transactions Act and pushed out to the financial institution world by no less than six federal agencies, including a 59-page set of rules from the NCUA. The Red Flag program lays out a list of requirements that carry a Nov. 1 deadline and that no financial institution can afford to ignore, a prominent compliance expert said.

"I tell my clients there are three things that are important to remember about Red Flag," said Sai Huda, CEO of Compliance Coach in San Diego, Calif.

"The first is do not underestimate the impact of complying with these. I'm seeing a lot of credit unions and other financial institutions just make the assumption that this is like other rules where you can just throw the policy together, get them approved and you're in compliance," he said.

"But it's not like that," said Huda, whose client list of several hundred financial institutions includes five of the 50 largest credit unions. "The Red Flag rules are quite complex and require a lot of work. For instance, you have to do a risk assessment of all the accounts that you offer consumers and then for each account, you have to look at the risk factors and decide if they need to be covered under the rules."

"And even if you decide they're not, you still have to account for them anyway, if there's a foreseeable risk of identity theft."

His second guidance to credit unions, Huda said, is to be aware of their "affirmative obligation." He explained that financial institutions under these rules now bear the onus of creating a program specifically designed to prevent identity theft.

"You can tell consumers to do their part, shred documents, don't open suspicious e-mails, that sort of thing, but this raises the bar again by telling credit unions that you have to do your part, too," Huda said. "It raises the bar."

The consequences of falling under that raised bar form Huda's third point.

"If a credit union fails to comply and doesn't have an adequate program in place, they can risk severe penalties," he said. Those can be in the form of liability under state and federal deceptive acts legislation or at the hands of an attorney who can sue the credit union after a breach and argue that it

Most Popular Articles

- 1 [Will CU Mortgage Market Go Into Reverse?](#)
 - 2 [Coalition a 'Stalking Horse' For Banks, Association's Argue](#)
 - 3 [New Player Enters CU Prepaid Card Market](#)
 - 4 [CUs Have New Resource For Complying With Federal Credit Law](#)
 - 5 [Sterlent Credit Union Now Insolvent](#)
- » [Go to Complete List >>](#)



National CD Rateline

Highest
Jumbo
CD Rates
Period!

Buy Direct

Save
Thousands
in Fees

Free Trial

"America's
Favorite
Rate Board"

cdrateline.com
800-246-0005

didn't have an adequate identity theft program in place and that caused harm to members, Huda said.

The Red Flag program right now consists of 26 specific areas. One example is suspicious documents. Within that is a red flag that says financial institution staffers have to be aware when a photograph on an ID is not consistent with the appearance of the applicant or member actually in front of them.

And just as the number of accounts that a credit union might offer is growing—including everything from credit cards to checking to insurance and investments—so is the number of red flags.

Huda said the number his company is tracking, for instance, has just increased from 26 to 43 as the consultancy identifies more specific areas of possible compromise and fraud.

So how to keep up?

"Well, the government has limited resources, so it's telling credit unions to go find their own resources," Huda said. His company is aiming to get involved in that business opportunity by offering CompliancePal, an online compliance monitoring and alert service that starts at \$295 a year for credit unions of \$165 million or less in assets.

Other vendors are getting involved, too. For instance, PM Systems Corp., a South Carolina-based provider of e-commerce and security solutions to dozens of credit unions, is offering a suite of enhancements to its online banking suite.

That includes monitoring systems through a back-office console that "permits thresholds to be established along with granular control of alert functions," said the company's vice president, Robert Broadwell.

He said his company also has developed an "extended set of violation procedures we call Red Flag Pass that provide more thorough validation of first-time online banking users, membership enrollments and address changes."

While Broadwell said the Red Flag program in general "places yet another needless compliance burden on credit unions, don't blame the NCUA. They're just the messenger from the congressional promulgators on high."

He said his reading of the NCUA rules found them to be "vague and ambiguous with phrases like 'appropriate' and 'reasonably foreseeable' and 'reasonable policies,'" a result, he said, of the need for "argument wiggler room that was intentionally introduced as a result of comments from those that weighed in during the regulatory comments period."

That said, there is some method to this madness.

"The single most important functional goal of Red Flag is to provide members with a very timely and effective means of dealing with an identity theft incident," Broadwell said.

"This is a tangible goal that can be positively accomplished with minimal effort. The other component goals such as detection and prevention are more elusive because most data processing systems are not as equipped," he said.

The PM Systems executive also had some specific advice for credit unions as the Nov. 1 deadline approaches.

"If you don't do anything else about Red Flag, make sure you have conducted a Red Flag risk assessment and completed your written Red Flag program," Broadwell said.

"You also need to make sure you have addressed each part of Appendix J and gotten involvement and documented ratification from senior management and your board of directors," he said.

Despite whatever identity theft software and policies are in place, the Red Flag program "is all about the paperwork," Broadwell said.

"Remember that. If you miss that November date, at least make sure you have those things done before your examiner shows up."

—mrapport@sc.rr.com

» [View the May 07, 2008 Issue of Credit Union Times](#)



[Industry Links](#) [About Us](#) [Privacy Policy](#) [Site Map](#) [Advertising Information](#)

(c) 2008 *Credit Union Times*. A Highline Media publication. All rights reserved.
www.highlinemedia.com | www.summitbusinessmedia.com
