



HEALTHCARE AND FINANCIAL SERVICES REGULATORY REFORM aren't the only things happening in Washington. Federal regulators have been busy issuing and delaying new rules governing identity theft, financial privacy and health privacy.

Red flags rule for identity theft is delayed until June. In November 2007, the Federal Trade Commission issued the "Red Flags Rule," which requires certain businesses to develop and implement written programs for preventing and detecting identity theft. The FTC delayed enforcement until June 2010.

Under the rule, creditors must adopt programs that provide for the identification, detection and

has no covered accounts must periodically conduct a risk assessment to help determine if it has acquired any covered accounts through changes to its business structure or processes.)

The House of Representatives recently approved a bill allowing the Federal Trade Commission to exempt businesses that can establish they (a) know all their customers/clients individually, (b) only perform services in or around the residences of its customers, or (c) have not experienced episodes of identity theft and/or identity theft is rare for their type of business.

Model notices for financial privacy are adopted. On another front, federal financial services regulators have published a model privacy notice that financial institutions can adopt to comply with the Gramm-Leach-Bliley Act financial privacy rules. The two-page model notice tries to encourage simpler, clearer privacy notices that enable consumers to easily compare privacy information-sharing practices. A notice must explain an institution's policies and practices for disclosing nonpublic personal information and give consumers an opportunity to opt out. Previous efforts at privacy notices were deemed too confusing.

To use the model, an institution can simply insert its name on a government online form and pick and choose from a menu of options to identify the types of information it collects and shares. One version of the notice does not include an opt-out option. Another explains how to opt out of data sharing by telephone and online. A third includes a mail-in opt-out form. Use of the model notice is not required, but financial institutions that do will benefit from a safe harbor.

State regulators have not adopted the model notice, nor have they indicated whether they will follow the federal lead. So, before using

the model notice, industry players subject to GLBA privacy rules should make sure they comply with relevant state requirements.

GINA rules! The Genetic Information Nondiscrimination Act (GINA) was enacted 18 months ago with the intent of protecting individual genetic information from being used to discriminate in health insurance and employment. Health insurers cannot deny coverage or charge higher premiums to a person based on genetics and the possibility that genetics indicate that person might develop a disease in the future.

The law also prohibits employers from using genetic information when making personnel decisions. The law applies to employers with 15 or more employees and prohibits them from intentionally acquiring genetic information about applicants and employees. The law prohibits an employer from asking about family medical history during an interview or after an employee is hired.

The health insurer provisions took effect in May; the employer provisions in November. Most recently, the Departments of Treasury, Health and Human Services, and Labor issued joint regulations implementing Title I, which prohibits employer-sponsored group health plans and health insurers from restricting enrollment or adjusting premiums based on genetic information or requiring or requesting genetic testing. The regulations have caused some controversy because of their potential impact on gathering information for wellness and similar programs. Although it appears the established structure is workable, the issue serves as a warning that GINA's reach may be wider than anticipated.

Regs Rule!

While you were monitoring health-care reform, the bureaucracy was quietly going about its business. ID theft, financial privacy and health privacy changes could affect you.

response to patterns, practices or specific activities that indicate the possibility of identity theft. Red flags may include unusual account activity, fraud alerts on a consumer report, or an attempted use of suspicious account application documents. Programs must describe appropriate responses that would prevent and mitigate the crime and detail a plan to update the program.

The rule applies to all creditors who have "covered accounts." A creditor includes any entity that extends credit on a regular basis or arranges for others to do so. Creditors also include entities that regularly permit deferred payments for goods or services. A covered account is defined as a consumer account that is designed to allow multiple payments or transactions, or any account where there is a risk of identity theft.

This raises a question for insurance brokers. Are they considered creditors with covered accounts? Are they required to comply?

It appears unlikely many will fall within the rule, but producers who also act as investment advisors or provide other credit-like services to clients should take a closer look. (A business that could be a creditor but

SINDER, A PARTNER AT STEPTOE & JOHNSON, IS CIAB GENERAL COUNSEL. ssinder@steptoe.com FIELDING IS OF COUNSEL AT STEPTOE & JOHNSON. jfielding@steptoe.com