UNC SCHOOL OF GOVERNMENT

HEALTH LAW BULLETIN NUMBER 89 | NOVEMBER 2008

The Federal Identity Theft "Red Flag" Rules and North Carolina Local Health Departments

Jill Moore

In November 2007, several federal agencies jointly issued a new set of regulations intended to help prevent, detect, and mitigate identity theft. The regulations, known as the identity theft "red flag" rules, require the entities they cover to develop policies and procedures to recognize and respond to circumstances that may indicate identity theft has occurred.

The rules apply to financial institutions and *creditors*—a term that is defined to include public and private service providers that allow their clients to defer payment for services received. Although we do not ordinarily think of local health departments as creditors, this definition picks up health departments that allow their clients to receive services and pay for them at a later date. Such health departments are subject to the red flag rules and need to take several specific actions no later than May 1, 2009.

If it determines it is subject to the rules, the key actions that a health department must take are:

- Determine which of its accounts are *covered accounts*, as defined by the rules.
- Develop and implement a written identity theft prevention (ITP) program with policies and procedures in areas specified by the rules.
- Obtain administrative approval of the ITP program.
- Train appropriate staff members to implement the ITP program.
- Provide for the continuing administration of the ITP program.

This bulletin addresses several frequently asked questions about the red flag rules and their application to North Carolina local health departments.

Jill Moore is a School of Government faculty member who specializes in public health law.

1. First, some background information: Where did these rules come from, when are they effective, and where can local health departments obtain a copy?

The red flag rules were adopted to implement portions of the Fair and Accurate Credit Transactions Act of 2003 (the FACT Act).[1] The term "red flag rules" encompasses a set of rules that were jointly issued by several federal agencies, but the particular rules that are of interest to local health departments are overseen by the Federal Trade Commission (FTC). The rules were published in November 2007 and became effective January 1, 2008.[2] The original mandatory compliance date was November 1, 2008. However, in late October 2008, the FTC announced that compliance will not be enforced until May 1, 2009.[3] The FTC's portion of the rules is contained in Part 681 of Title 16 of the Code of Federal Regulations. The Federal Register notice with the final rules and some explanatory commentary is available on the Internet at http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf.

2. Do the red flag rules apply to local health departments?

If a local health department provides services for which clients are allowed to defer payment, then it is subject to the rule that requires entities to establish an identity theft prevention (ITP) program for any *covered accounts* they maintain.[4] This rule creates duties for *creditors*, which is defined to include any government agency that "regularly extends, renews, or continues credit."[5] *Credit* is defined to include the purchase of services for which payment is deferred.[6] Thus, the FTC has interpreted the term creditor to include private and governmental service providers—including public health departments[7]—if they allow individuals to defer payment for services.

3. If a local health department meets the definition of creditor, what must it do next?

A health department that meets the definition of creditor must determine (and periodically redetermine) whether it maintains or offers *covered accounts*.[8] The term *covered account* is defined to include:

> "(i) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, … and

1. Pub. L. No. 108-159, 117 Stat. 1952 (2003).
2. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003, 72 Fed. Reg. 63718 (Nov. 9, 2007).
3. Federal Trade Commission, FTC Will Grant Six-Month Delay of Enforcement of "Red Flags" Rule Requiring Creditors and Financial Institutions to Have Identity Theft Prevention Programs (Oct. 22, 2008), http://www.ftc.gov/opa/2008/10/redflags.shtm.
4. 16 C.F.R. § 681.2. There are two other sections of the red flag rules that are not addressed in this bulletin. Section 681.3 applies only to issuers of credit or debit cards. Section 681.1 applies to entities that use consumer reports to check the credit history of employees or customers to whom credit will be extended. Entities subject to section 681.1 must develop and implement reasonable policies and procedures to respond when a consumer report sends the entity a notice of address discrepancy. If a local health department uses consumer reports, it should review section 681.1 to determine the scope of its obligations.
5. *Id.* § 681.2(b)(5).
6. *Id.* § 681.2(b)(4).
7. Telephone interview with Tiffany George, Attorney, Federal Trade Commission Division of Privacy and Identity Protection (Oct. 22, 2008).
8. 16 C.F.R. § 681.2(c).

> (ii) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from identity theft, including financial, operational, compliance, reputation, or litigation risks."[9]

An *account* is defined as "a continuing relationship established by a person with a financial institution or creditor to obtain a product or service for personal, family, household, or business purposes."[10]

There are two steps to determining which, if any, of a health department's accounts are covered accounts. First, the department should determine whether any of the accounts it maintains fit within part (i) of the definition of covered account. For example, an account for a family planning client would likely fit within this part of the definition, because family planning accounts typically are designed to permit multiple payments. Second, the department should consider whether any of its accounts fit within part (ii) of the definition. In making this determination, the rules require the department to conduct a risk assessment that takes into account the methods used to open accounts, the methods provided for access to accounts, and the department's previous experiences with identity theft.[11] The rules do not elaborate on how such a risk assessment should be done. However, the preamble to the final rule explained that creditors should consider factors such as whether accounts may be opened or accessed remotely, such as by telephone or through the internet.[12]

If a local health department has any accounts that satisfy either part of the definition, then it maintains covered accounts.

4. If a local health department determines it maintains covered accounts, what must it do?

After determining which of its accounts are covered accounts, the department must:

1. Develop and implement a written identity theft prevention (ITP) program designed to detect, prevent, and mitigate *identity theft*.[13] The program must be appropriate to the size and complexity of the department and the nature and scope of its activities, and include reasonable policies and procedures to:

    - Identify *red flags*—defined as patterns, practices, or specific activities that indicate the possible existence of identity theft.
    - Detect red flags when they occur.
    - Respond appropriately to any red flags that are detected, to prevent and mitigate identity theft.
    - Ensure that the ITP program is updated periodically to reflect changes in risks to clients and to the safety and soundness of the department.

9. *Id.* § 681.2(b)(3).
10. *Id.* § 681.2(b)(1).
11. *Id.* § 681.2(c).
12. 72 Fed. Reg. at 63724.
13. 16 C.F.R. § 681.2(d). *Identity theft* is defined as "a fraud committed or attempted using the identifying information of another person without authority." *Id.* § 681.2(b)(8) (incorporating by reference the definition in 16 C.F.R. § 603.2(a)). *Identifying information* means "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," and includes (among other things) name, social security number, date of birth, driver's license or other government-issued identification number, and taxpayer identification number. *Id.* § 603.2(b).

- In developing its ITP program, the health department must consider guidelines developed by the FTC and published as Appendix A to the regulations, and it must incorporate the guidelines into its program when appropriate.[14]

2. Obtain approval of the initial written ITP program from the department's *board of directors* or an appropriate committee of the board of directors.[15] For health departments, this probably means the board of health.[16]
3. Involve the board of directors, an appropriate subcommittee of the board, or a designated employee at the level of senior management in the oversight, development, implementation and administration of the program.[17] For health departments, this function could be served by the board of health, or by the health director or another high-level administrator within the department.
4. Train staff, as necessary, to effectively implement the program.[18]
5. Exercise appropriate and effective oversight of service provider arrangements.[19] This portion of the rule applies when a creditor uses a third-party service provider to carry out activities in which identity theft red flags may be detected. In this situation, a creditor "should take steps to ensure that the activity of the service provider is conducted in accordance with reasonable policies and procedures to detect, prevent, and mitigate the risk of identity theft."[20] A local health department that has these types of service provider arrangements should consider including a provision in its contract with the service provider that addresses this issue and explains how the department expects the provider to respond to any red flags it detects. For example, a health department could require a service provider to report the red flags to the health department, or it could permit the provider to respond according to its own policies and procedures.[21]
6. Provide for the continuing administration of the program.[22]

5. What constitutes a red flag that must be addressed in the ITP program?

The rules define a red flag as "a pattern, practice, or specific activity that indicates the possible existence of identity theft."[23] As noted above, in developing its ITP program, a health department must consider FTC guidelines contained in Appendix A to the rules. The portion of the appendix

14. *Id.* § 681.2(f); *see also* Interagency Guidelines on Identity Theft Detection, Prevention, and Mitigation, 16 C.F.R. pt. 681, app. A.
15. *Id.* § 681.2(e)(1).
16. This is a bit unclear because the regulation's definition of *board of directors* does not actually define the term for creditors such as health departments. Instead, it states that for creditors who do not have a board of directors, the term includes "a designated employee at the level of senior management." 16 C.F.R. § 681.2(b)(2). Still, it seems it would be reasonable to conclude that the board of health is the board of directors for purposes of this regulation, since it is the policy-making body for the department under North Carolina law. See N.C. Gen. Stat. §§ 130A-35 (county boards of health); 130A-37 (district boards of health); 130A-43 (consolidated human services board); 130A-45.1 (public health authority board).
17. 16 C.F.R. § 681.2(e)(2).
18. *Id.* § 681.2(e)(3).
19. *Id.* § 681.2(e)(4).
20. *Id.* pt. 681, app. A, section VI.
21. See *id.* pt. 681, app. A., section VI, subsection (c).
22. *Id.* § 681.2(e).
23. *Id.* § 681.2(b)(9).

that addresses how to identify red flags divides the matters to be considered into three groups: risk factors, sources of red flags, and categories of red flags.
Departments must consider the following risk factors in identifying relevant red flags:

- The types of covered accounts the department offers or maintains,
- The methods the department provides to open covered accounts,
- The methods the department provides to access covered accounts, and
- The department's previous experiences with identity theft.

In addition, departments must consider the following sources of red flags:

- Incidents of identity theft that the department has experienced,
- Methods of identity theft that the department is aware of and that reflect changes in identity theft risks, and
- Applicable supervisory guidance.

Finally, the department should include relevant red flags that appear in several categories specified in the appendix. Some categories appear unlikely to apply to local health departments, but each department should make that determination for itself, based on the types of covered accounts it maintains and its experiences with managing those accounts. A supplement to the appendix provides examples of each category. The following list includes only those examples that seem particularly likely to be relevant to local health departments, so departments should consult the full list in developing their programs:

- *Alerts, notifications, or other warnings received from consumer reporting agencies or service providers.* This category will probably be of interest only if the local health department receives consumer reports on its clients.
- *The presentation of suspicious documents.* Examples of suspicious documents include identification documents that appear altered or forged, applications that appear altered or forged, a photo or physical description on an identification document that is not consistent with the appearance of the client who provides it, or other information on an identification document that is not consistent with information the health department already has on file.
- *The presentation of suspicious identifying information.* Examples include personal identifying information that is inconsistent with information from external sources available to the health department, personal identifying information that is inconsistent with other personal identifying information provided by the same client, a social security number that is the same as the SSN presented by another client, and personal identifying information that is not consistent with the personal identifying information the department has on file for the client.
- *The unusual use of, or other suspicious activity related to, a covered account.* The examples in this category appear to apply primarily to entities that offer credit cards or other financial accounts, and to utilities.
- *Notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts.* The sole example in the supplement describes a circumstance in which the department is notified that it has opened a fraudulent account for a person engaged in identity theft.

6. How must a health department respond when it detects red flags?

Health departments' ITP programs must include policies and procedures for responding to red flags, in order to prevent or mitigate identity theft.[24] The appendix to the red flag rules states that policies and procedures should be appropriate and commensurate with the degree of risk the particular red flag creates, and it offers the following examples of responses that may be appropriate, depending on the circumstances.

- Monitoring a covered account for evidence of identity theft;
- Contacting the customer;
- Changing passwords, security codes, or other security devices that permit access to the account;
- Reopening a covered account with a new account number;
- Not opening a new covered account;
- Closing an existing covered account;
- Not attempting to collect on a covered account or not selling a covered account to a debt collector;
- Notifying law enforcement; or
- Determining that no response is warranted under the particular circumstances.

Some of these examples seem more likely to be applicable to financial accounts than to health department accounts, but each health department should consider the full list and determine for itself whether a particular example might constitute an appropriate response in some circumstances—and if so, what those circumstances are. Also, in developing policies and procedures for responding to red flags, departments should remember that all aspects of the ITP program must be appropriate to the nature and scope of the department's activities.[25] See the next question for some special considerations that health departments should keep in mind when determining what types of responses are appropriate for them.

7. Are there special considerations for local health departments in developing their ITP programs?

Yes, there are at least three: (1) health departments' obligation to comply with medical confidentiality laws; (2) their obligation to comply with nondiscrimination laws; and (3) their role as a provider of essential public health services. There may also be other special considerations arising from particular programmatic requirements or other sources.

Medical confidentiality. In developing their policies and procedures for responding to red flags, health departments must keep in mind that any responses they develop that involve the disclosure of individually identifiable health information must comport with any applicable confidentiality laws. At a minimum, individually identifiable information about clients in clinical programs will be subject to both the HIPAA medical privacy rule[26] and state confidentiality laws, [27] and some

24. *Id.* § 681.2(d)(2)(iii).
25. *Id.* § 681.2(d)(1).
26. 45 C.F.R. pts. 160 and 164.
27. A handout with some of the state medical confidentiality statutes that apply to N.C. local health departments is available at http://www.sog.unc.edu/programs/ncphl/ReqsForConfMedInfo/Confid%20Statutes%20May%2008.pdf.

programs may be subject to other confidentiality requirements as well. Responses to red flags should not involve disclosures of such information unless the disclosures are permitted under all applicable confidentiality laws.

Nondiscrimination laws. As recipients of federal financial assistance, health departments must comply with Title VI of the federal Civil Rights Act, which prohibits discrimination on the basis of race, color, or national origin.[28] Any policies and procedures developed for the ITP program should not single out any of these groups for differential treatment. In addition, departments must not adopt policies and procedures that have the effect of denying or impeding services to any of these groups, even if those policies and procedures are not intended to treat the different groups differently.

Providing essential public health services. Another consideration for health departments is their core mission of protecting the public health, which is achieved in part through services to individuals.[29] Local health department staff members know from experience that some clients provide false names or present false identification, for a variety of reasons. The presentation of false identification is likely to constitute a red flag for purposes of the ITP program. However, this is a red flag that health departments have discretion in responding to, and their response should not be structured in a way that denies services to individuals who are otherwise eligible for them,[30] or that undermines the department's ability to protect the public health.

8. Must a county health department have its own ITP program, or may it be covered by a countywide program?

The regulations do not directly address this question. According to an FTC staff attorney, either approach is permitted under the regulations. However, a countywide program must address differences in the different departments covered by the program.[31] For example, if a county covers utilities as well as the health department in its program, then it needs to have different policies and procedures that are tailored to the different agencies.

28. 42 U.S.C. § 2001d; *see also* 45 C.F.R. § 80.3 (regulations implementing Title VI).

29. *See* N.C. Gen. Stat. § 130A-1.1 (describing the mission of North Carolina's public health system and defining the essential public health services that state public health agencies must attempt to ensure are available and accessible throughout the state).

30. Telephone interview with Tiffany George, Attorney, Federal Trade Commission Division of Privacy and Identity Protection (Oct. 22, 2008). Ms. George's particular comment addressed the provision of services to immigrants, who are generally eligible for North Carolina local health department services regardless of their immigration status. *See generally* Jill D. Moore, Noncitizen Eligibility for N.C. Local Health Department Mandated Services, http://www.sog.unc.edu/programs/ncphl/ImmigrantHealth/Eligibility-LHDservices.pdf.

31. Telephone interview with Tiffany George, Attorney, Federal Trade Commission Division of Privacy and Identity Protection (Oct. 22, 2008).

To browse a complete catalog of School of Government publications, please visit the School's website at www.sog.unc.edu or contact the Publications Division, School of Government, CB# 3330 Knapp-Sanders Building, UNC Chapel Hill, Chapel Hill, NC 27599-3330; e-mail sales@sog.unc.edu; telephone 919.966.4119; or fax 919.962.2707.