



Eligibility Test for Red Flag

The following Information is intended to be factual and authoritative in regard to the subject matter referenced; however, by virtue of this publication, we are not providing legal, accounting or other professional advice for specific companies or financial institutions. We do not guarantee nor imply that we can provide compliance with any state or federal law or regulation. Please consult with your legal or compliance advisor before taking any action on information contained herein. – Aegis Identity Protect and NXG Strategies, LLC

Copyright 2008-2009 NXG Strategies, LLC – All Rights Reserved

Instructions: Read the questions below. Check the box if the answer to the question is “YES.” If you can check off any of the boxes, then you are probably subject to the Red Flag Rules and must have your own written Red Flag Plan.

1. Are you any of these?

- Physician or Surgeon
- Medical Clinic
- Dentist
- Chiropractor
- Dietician or Nutritionist
- Podiatrist
- Therapist
- Veterinarian
- Clinical Laboratory Facility providing services to the public
- Diagnostic Facility providing services to the public
- Emergency Medical Facility
- Health and Wellness Facility
- Hospital
- Other Person or Organization who provides goods or services to consumers

2. Do you or your organization fit the definition of “Creditor” shown below?

“Any person or business who arranges for the extension, renewal, or continuation of credit”. In a clarification provided by the Federal Trade Commission, an organization would be included in the definition of “creditor” if the organization does not regularly demand payment in full for goods or services at the time that such goods or services are delivered

4. If you are not sure about Questions 1 and 2, ask these questions:

_____ “If a criminal uses a false or stolen identity to participate in my products or services, could it result in a financial loss to a consumer or business, either through a transaction that I initiate, or a transaction that I validate that is initiated down the line by someone else?”

_____ “If a criminal uses a false or stolen identity to participate in my products or services, could it result in any harm to a consumer or business, either within my organization or through the products and services that I provide (such as medical records contamination, false arrest, loss of credit status, loss of government benefits, delay of payment of insurance benefits, etc.)?”

_____ “Are the products or services that I provide considered “validation” for obtaining other products or services, and by virtue of this fact, we could be abetting identity theft in another organization (such as a relationship with a physician that is used to validate services with diagnostic services, laboratories, hospitals, etc.)?”

RESULT OF TEST:

_____ If you checked any of the boxes “YES”, then you are probably subject the Red Flag rules of FACTA Section 114)

_____ If you did NOT check any boxes, and you are a health care organization, then you should consult with your legal advisor or governing agency regarding a final determination of whether or not you are subject to the FACTA Section 114.

Defining Additional Red Flags

If you don't know how to determine what your Red Flags might be, answer these questions:

1. How would I find out if a person were posing as a fictitious person (using bogus identification) to gain access to products or services with the intent of defrauding our organization?
2. How would I find out if a person were posing as someone else, using valid identification belonging to another person?

One very important consideration is to remember is that you can not rely on paper documents alone as a means of identification. With the sophistication and the easy access to computer software and printers, any criminal can forge a driver's license, state ID, birth certification, and other documents normally relied upon for identification.

RESULT OF TEST: The answers to these questions should point to the needed detection methods that you will put in place in order to detect identity theft before or after it occurs. All of the possible outcomes of the detection, with the exception of the desired outcome, become your red flags.

Identifying Covered Accounts

If you don't know which accounts in your organization are covered accounts, try looking at your Income Statement. For each line of revenue ask (check if answer is "yes"):

1. "To generate this revenue, do we defer payment in full until after the time of service?" If yes, then this is probably a covered account. Confirm with the second question below. If payment in full is collected before or at the time that service is performed then this may NOT be a covered account.
2. "Is it possible for a consumer to obtain this product or service and default on the payment?" If yes, then this is probably a covered account.
3. "Can a criminal establish this type of account for the purpose of validating their identity, resident status, insurance status or other criteria that may be relied upon by others to establish a covered account elsewhere?" If yes, then this is probably a covered account under the second part of the definition, which states that a covered account is also any account for which there is a reasonable foreseeable risk of identity theft." (Example – Establishing an account with a physician in order to validate a relationship with other medical services organizations or hospitals. See Footnote)

RESULT OF TEST: If you answered "YES," then you have possibly identified a covered account that should be part of your Red Flag Program. The spirit and purpose of the regulation is to try to stop identity theft at one of the points of vulnerability - the point at which a financial transaction takes place in exchange for goods and services. It also is acknowledged in FACTA Section 114, that while this regulation focuses on financial transactions, medical organizations also have a duty to protect the accuracy and privacy of medical records.

FOOTNOTES

EXCERPTS from FACTA Section 114 63718 Federal Register / Vol. 72, No. 217 / Friday, November 9, 2007 / Rules and Regulations

§ __.90(b)(10) **Service Provider.** The proposed regulations defined "service provider" as a person that provides a service directly to the financial institution or creditor. This definition was based upon the definition of "service provider" in the Information Security Standards. One commenter agreed with this definition. However, two other commenters stated that the definition was too broad. They suggested narrowing the definition of "service provider" to persons or entities that have access to customer information.

Section __.90(b)(10) of the final rules adopt the definition as proposed. The Agencies have concluded that defining "service provider" to include only persons that have access to customer information would inappropriately narrow the coverage of the final rules. The Agencies have interpreted section 114 broadly to require each financial institution and creditor to detect, prevent, and mitigate identity theft not only in connection with any existing covered account, but also in connection with the opening of an account. A financial institution or creditor is ultimately responsible for complying with the final rules and guidelines even if it outsources an activity to a third-party service provider. Thus, a financial institution or creditor that uses a service provider to open accounts will need to provide for the detection, prevention,

and mitigation of identity theft in connection with this activity, even when the service provider has access to the information of a person who is not yet, and may not become, a “customer.”

The Information Security Standards define “service provider” to mean any person or entity that maintains, processes, or otherwise is permitted access to customer information or consumer information through the provision of services directly to the financial institution. 12 CFR part 30, app. B (national banks); 12 CFR part 208, app. D-2 and part 225, app. F (state member banks and holding companies); 12 CFR part 364, app. (state non-member banks); 12 CFR part 570, app. B (savings associations); 12 CFR part 748, App. A (credit unions).

§ __.90(b)(3) Covered Account. As mentioned previously, the Agencies have added a new definition of “covered account” in § 1.90(b)(3) to describe the type of “account” covered by the final rules. The proposed rules would have provided a financial institution or creditor with broad flexibility to apply its Program to those accounts that it determined were vulnerable to the risk of identity theft, and did not mandate coverage of any particular type of account.

Consumer group commenters urged the Agencies to limit the discretion afforded to financial institutions and creditors by requiring them to cover consumer accounts in their Programs. While seeking to preserve their discretion, many industry commenters requested that the Agencies limit the final rules to consumer accounts, where identity theft is most likely to occur.

The Agencies recognize that consumer accounts are presently the most common target of identity theft and acknowledge that Congress expected the final regulation to address risks of identity theft to consumers.¹³ For this reason, the final rules require each Program to cover accounts established primarily for personal, family or household purposes, that involve or are designed to permit multiple payments or transactions, *i.e.*, consumer accounts. As discussed above in connection with the definition of “account,” the final rules also require the Programs of financial institutions and creditors to cover any other type of account that the institution or creditor offers or maintains for which there is a reasonably foreseeable risk from identity theft.

Accordingly, the definition of “covered account” is divided into two parts. The first part refers to “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.” The definition provides examples to illustrate that these types of consumer accounts include, “a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account.”

The second part of the definition refers to “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.” This part of the definition reflects the Agencies’ belief that other types of accounts, such as small business accounts or sole proprietorship accounts, may be vulnerable to identity theft, and, therefore, should be considered for coverage by the Program of a financial institution or creditor.

In response to the proposed definition of “account,” a trade association representing credit unions suggested that the term “customer” in the definition be revised to refer to “member” to better reflect the ownership structure of some financial institutions or to “consumer” to include all individuals doing business at all types of financial institutions. The definition of “account” in the final rules no longer makes reference to the term “customer”; however, the definition of “covered account” continues to employ this term, to be consistent with section 114 of the FACT Act, which uses the term “customer.” Of course, in the case of credit unions, the final rules and guidelines will apply to the accounts of members that are maintained primarily for personal, family, or household purposes, and those that are otherwise subject to a reasonably foreseeable risk of identity theft.