D. Designing Your Identity Theft Prevention Program

1. **Do creditors or financial institutions have to develop an Identity Theft Prevention Program if they already comply with data security requirements like the Health Insurance Portability and Accountability Act (HIPAA) or the Gramm-Leach-Bliley Act (GLB)?**

   Yes. The FTC strongly encourages reasonable data security practices, but the Red Flags Rule is not a data security regulation. Good data security practices — like collecting only the personal information you need, protecting that information, and securely disposing of what you no longer need — help ensure that personal information does not fall into the hands of identity thieves. For more on data security, visitwww.ftc.gov/infosecurity.

   Â The Red Flags Rule picks up where data security leaves off. If identity thieves do get hold of someone's personal information, they typically use it to get goods or services from unsuspecting businesses and have no intention of paying the bill. By having companies set up procedures to look for and respond to the "red flags" that an identity thief is trying to use someone else's information, the Rule seeks to reduce the damage crooks can inflict both on victims of identity theft and on businesses left with accounts receivable they'll never be able to collect. While you may be able to incorporate some of your data security practices, your Identity Theft Prevention Program is a different kind of plan aimed at preventing a different kind of harm.

2. **Does the Rule require that I have specific practices or procedures in my Program — like identifying a particular red flag or reporting suspected identity theft?**

   The Rule doesn't require any specific practice or procedures. It gives you the flexibility to tailor your Program to the nature of your business and the risks it faces. The FTC will assess compliance based on the reasonableness of a company's policies and procedures. Businesses with a high risk for identity theft may need more robust procedures — like using other information sources to confirm the identity of new customers or incorporating fraud detection software. Groups with a low risk for identity theft may have a more streamlined Program — for example, simply having a plan for how they'll respond if they find out there has been an incident of identity theft involving their business. The FTC has designed aform to help groups at low risk for identity theft put together a Program. It's available atwww.ftc.gov/redflagsrule.

3. **Does the Red Flags Rule require me to check photo IDs of my customers? If I check photo IDs, should I keep copies?**

   The Rule doesn't specifically require you to check customers' photo IDs. Of course, for some businesses, checking photo IDs is one way to verify that customers are who they claim to be. But if you decide to ask for a photo ID, keeping a copy often is unnecessary and can raise privacy and data security concerns, especially if you're collecting other personal information like date of birth, address, or Social Security number.

D. Designing Your Identity Theft Prevention Program (Continued)

4. **Does the Red Flags Rule require that I use Social Security numbers to verify my customers' identity?**
   No, the Red Flags Rule does not require that you use Social Security numbers or any other specific identifying information. Whether you collect Social Security numbers or other information to verify a customer's identity depends on the nature of your business and the risks you face. Actually, collecting a Social Security number by itself is not a reliable way to verify someone's identity because the numbers are widely available and do not prove a person is who he or she claims to be. However, Social Security numbers can be helpful as part of a more comprehensive identity verification process — for example, as a way to check against information from other sources or as a way to get other information, like a credit report, which can be used to verify a person's identity.

   It's a good data security practice not to collect more information than you need. If you are asking for a Social Security number, but not actually using it as part of a more comprehensive authentication process, reconsider whether your business really needs to collect and maintain it.

5. **How do my obligations under other laws affect the implementation of my Identity Theft ?**
   Your Program under the Red Flags Rule should be consistent with other relevant legal, professional, and ethical obligations. This would include laws relating to the provision of medical treatment or the provision and termination of utility services. Indeed, the Rule anticipates the need to accommodate obligations like these by requiring that a Program include only "reasonable" policies and procedures, and by ensuring that each group has the flexibility to tailor a Program to the nature of its business.

6. **Under what circumstances should I contact law enforcement? Who handles identity theft?**
   If your business or organization experiences a confirmed incident of identity theft, it's a good idea to report it to law enforcement. Your local police department would be a good place to start. If you suspect your business is being targeted specifically — say, by a persistent attack on your website — consider contacting the FBI or U.S. Secret Service. The FTC does not have jurisdiction to prosecute identity thieves, but it has many resources to help victims recover. Consider directing victims to the FTC's identity theft website,www.ftc.gov/idtheft.

7. **Are there samples or templates to help me set up my Program?**
   Yes. The FTC has created aform to help businesses at low risk for identity theft design a Program. It's atwww.ftc.gov/redflagsrule. Many trade associations have developed guidance to help industry members comply with the Rule, too. The FTC cannot recommend any particular vendor's compliance products or services.

8. **Is there a Red Flags certification or accreditation that will ensure our Program complies with the Rule?**
   No. Some companies and organizations offer Red Flags compliance services, but the FTC doesn't certify or approve any particular program. It's up to you to decide if you need help like that. Before paying for Red Flags compliance services, visitwww.ftc.gov/redflagsrule for free resources developed by the FTC to help you design your Program.

D. Designing Your Identity Theft Prevention Program (Continued)

9. **We're a creditor that regularly arranges for our customers to get credit from third parties and we have covered accounts. What should our Identity Theft Prevention Program look like?**
   You can create your own policies and procedures for your Program or incorporate reasonable policies and procedures from the lender's Program. Reasonable procedures might include asking for photo identification, comparing the photo to the person presenting the ID, looking for signs the ID has been altered or forged, and comparing the information on the ID with what's on the credit application. Your Program also should include reasonable procedures for responding to red flags and complying with the Rule's administrative requirements.

10. **Does the FTC have a sample training policy for employees?**
    No. That wouldn't be practical because each Program is unique. Your employee training policies should be based on the specific red flags you've identified in your business or organization and the procedures you've put in place for detecting and responding to those red flags.

11. **What if we hire service providers? If our business has to have a Program under the Rule, do our service providers need a Program, too?**
    It depends on what they're doing for your business. There are generally two types of service providers you'll need to supervise under the Rule. First, there are service providers in the business of fraud detection who help identify, detect, and respond to red flags. If you hire a company like that, you must make sure it's meeting the same standards that would apply if you were doing those things yourself.

    Second, other companies you hire may not be in the business of fraud detection, but will be the only ones who can detect the red flags you've identified in your Program. For example, a debt collector you use to contact customers about outstanding debts may hear from consumers who have been the victims of identity theft. Certainly, if you were performing that task yourself, you'd spot that as a red flag. Since you've hired a debt collector, you must ensure that they either comply with your Program or have their own policies and procedures to detect and respond to red flags. Under the Red Flags Rule, you do not need to supervise service providers who merely have access to data about your customers, but aren't in a position to detect the red flags in your Program — like janitorial contractors or certain types of software support providers. For more about service providers, read *Fighting Fraud with the Red Flags Rule: A How-To Guide for Business*, atwww.ftc.gov/redflagsrule.