

Q Are there sample policies and procedures to get us started?

A While there are probably sample policies and procedures readily available on the Internet, the Red Flags Rule requires the Identity Theft Prevention Program be tailored to each specific "creditor" based on the nature and complexity of the creditor's business.

Q Should we request a Social Security number (SSN) on job applications or should we follow up with a separate document?

A From a record retention standpoint, it would be easier to simply request a Social Security number on the job application so the employer would have fewer records to maintain. The bigger issue, however, is the need to protect information regardless of the route you choose and the medium in which such information is retained.

Q Is the Red Flags Rule applicable to CPA firms?

A That depends on the types of accounts maintained by the CPA firm and the risk assessment performed. It is also worth noting that the Federal Trade Commission will be providing additional guidance for those businesses with a low risk of identity theft, such as businesses that know their customers personally. CPA firms may fall into this category.

Q Can we print the PowerPoint slides from the webcast? Can this be incorporated as a part of our *Health Insurance Portability and*

Accountability Act of 1996 (HIPAA) compliance program?

A Yes. The slides are available at <http://www.bkd.com/docs/industry/webcasts/RedFlagsPPT.pdf>.

Q Can you provide a link for the Red Flags Rules?

A The Red Flags Rule is available at: <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>.

Q Can you provide an example of how the Red Flags Rule applies to skilled nursing?

A If a skilled nursing center constitutes a "creditor" within the meaning of the Red Flags Rule, the provisions of the rule will apply. The center would need to conduct the risk assessment referenced in the rule and establish a written program to detect and mitigate any red flags associated with its patients' accounts. Given the prevalence of medical identity theft, this would involve setting up procedures to limit access to patients' records, etc. This can certainly be done in conjunction with any other policies already in effect pursuant to HIPAA or any other regulatory schemes.

Q Can you provide an example of how this rule would affect a non-profit foundation receiving contributions?

A It could possibly apply in situations where a non-profit foundation provides some type of benefit in

exchange for contributions or when the contributions are payable over time. For example, if the foundation provides monthly magazines or some other product or service in exchange for contributions made over time, the Red Flags Rule might apply.

Q Can you provide us with training for the risk assessment and audit tools?

A Yes. The training we can provide to your organization would be tailored to the scope and complexity of your operations.

Q Does the Red Flags Rule apply to a college that accepts credit cards?

A No. As the Federal Trade Commission has stated in some of its publications, the acceptance of credit cards alone would not trigger application of the Red Flags Rule.

Q For an independent school, payment plans may trigger compliance requirements. Must the plan cover grades/transcripts as well as financial information?

A The Red Flags Rule could potentially apply in those situations in which students are allowed to pay tuition over a period of time. In that event, the school's Identity Theft Prevention Program would need to cover access to student accounts that include certain types of information such as name, SSN, date of birth, electronic identification number, routing code, etc. With respect to grades/

transcripts, you would need to consult other statutory/regulatory provisions that may apply.

Q What do you recommend to staff of hospital emergency departments who suspect a patient is using another person's identity?

A The emergency department should treat the patient consistent with the legal obligations imposed by the *Emergency Medical Treatment and Active Labor Act of 1985*. However, you should also flag the records associated with that patient until it can be ensured the patient is who he/she claims to be. By doing this, you can safeguard the medical identity theft victim's records are not polluted with the records of the imposter.

Q What do hospitals need to do with business associates to be compliant? Who are our business associates?

A Hospitals should exercise effective oversight of any service provider that provides any type of service with respect to the hospitals' covered accounts. This can be accomplished via contracts that require the business associate to operate in accordance with its written Identity Theft Prevention Program and to promptly notify the hospital in the event of the detection of a red flag concerning a hospital account.

Q We are responsible to report annually to the board. What type of information should hospital's capture for this report?

A The report to the board should include the following: the effectiveness of the hospital's policies and procedures in addressing the risk of identity theft in connection with its covered accounts; the arrangements

with its service providers in relation to activities performed by the service providers on covered accounts; significant incidents involving identity theft as well as management's response to those incidents; and recommendations for material changes to the Identity Theft Prevention Program.

Q Where can I find the 26 red flags that are discussed in the Red Flags Rule?

A The red flags are available at: <http://www.ftc.gov/os/fedreg/2007/november/071109redflags.pdf>. You will find Appendix A on page 63,773. The 26 red flags are in Supplement A to Appendix A on page 63,774.

Q How can the consumer reporting agencies help with hospitals' compliance?

A A copy of a consumer report can help validate the identity of a person seeking employment with the hospital. A consumer report also contains information that can be used to validate the identity of a patient seeking medical attention.

Q How should we handle address returns from the post office?

A Mail returned by the post office because the intended recipient is no longer at that location can be a red flag indicating possible identity theft. This is particularly true when a utility service is still active at an address, yet the bill gets returned to the utility company. In that case, a follow-up telephone call to the customer may be warranted to determine if the customer has actually moved or completed a change of address request.

Q I work at a university. I just happened to be at our recreation sports center one day and found out someone can get a membership and photo ID without showing any other form of ID. As a result, I could use another student's name, my address and my picture for the cost of a membership. I realize this isn't a covered account since it's paid in full upfront but should this "gap" be fixed by requesting another form of ID to get the membership since the membership ID card has the potential of being used to gain greater access to other information in the victim's name?

A This is a definite gap that should be closed because it provides an easy opportunity for someone to obtain one form of photo identification that can be used later to either gain access to someone else's information or be used to obtain subsequent fraudulent identification.

Q I'm still having a difficult time seeing how someone might steal another's identity in a college setting as it relates to a covered account. I agree with the example you used of posting grades with SSNs. We don't use credit reporting agencies. Students apply for loans with banks, not with us. Do you have any other good college examples?

A Another example would be if a college allowed a student to pay his/her tuition over the course of the semester. In that instance, the college has extended "credit" to the student, thus triggering application of the Red Flags Rule. Another example would be if the student union or bookstore allowed a student to charge items and then subsequently billed the student for the amounts owed for those charged items.

Q **Is there a risk assessment tool that we can have access to?**

A There are risk assessment tools available commercially, however, most off-the-shelf solutions require adjustments in order to tailor the tool to your organization's needs. The six steps discussed in the Identity Theft Red Flags presentation provides a summary overview and framework of key considerations for performing a risk assessment.

Q **On the risk assessment form, would a hospital have only one type of covered account?**

A Not necessarily. One of the key reasons for performing a risk assessment is to identify all covered accounts and the risks associated with each type of account based on methods for opening accounts, methods for accessing established accounts and prior experience with identity theft. Depending on the complexity of your hospital's operations, you may identify a variety of covered accounts.

Q **We are a nonprofit organization and accept donations and pledges to be paid out in scholarships and grants. We do not access credit reports. Does this apply to us?**

A If no "credit" is being extended, the Red Flags Rule would not apply.

Q **We have already established policy and procedures. Is a written risk assessment required to be completed and documented?**

A While the Red Flags Rule does not require that the risk assessment itself be in writing, it would be advisable to have it in writing in order to have documentation of the foundation for the Identity Theft Prevention Program. This would also be true if an organization determined after performing the risk assessment that no written program is required. Documentation of such a conclusion would be vital in the event of an audit.

Q **What would be examples of third party service providers for college and universities? We've thought of our tuition payment plan company, our Perkins loan billing agency and the bookstore system, but I'm thinking there must be more we haven't thought of that could come within requirements of the Red Flags Rule.**

A Another example might be a software company that provides software development services that

require the company to have access to students' financial records. Another example might be an off site back-up storage company that has access to student records.

Q **Who would be the appropriate leader to head this up - accounting, audit, IT, risk manager?**

A A risk manager would possibly be an appropriate leader in addition to a privacy officer or compliance officer. Regardless of the person selected to oversee the day-to-day operation of the written program, there are two key points to remember: (1) the leader should be a member of senior management; and (2) the leader should be assisted in the development of the program by a committee consisting of a broad range of people from different departments.

This Q&A's content was written by qualified, experienced BKD professionals, but applying specific information to your situation requires careful consideration of facts and circumstances. Consult your BKD advisor before acting on any matter covered in this update.

For more information please contact your BKD advisor or visit our website at www.bkd.com.