UNIVERSITY OF MICHIGAN
FINANCE

RED FLAG RULES
FREQUENTLY ASKED QUESTIONS

Ann Arbor, MI – October 16, 2009

Question 1: *What are "Red Flag Rules?"*

Answer 1: Red Flag Rules require businesses that loan customers money, accept payments, or use credit reports to have methods in place to detect and prevent identity theft.

Question 2: *Are the Red Flag Rules part of a law?*

Answer 2: The Red Flag Rules are part of the Fair and Accurate Credit Transactions Act (FACTA), an amendment to the 2003 Fair Credit Reporting Act., which is a federal law. FACTA is designed to prevent identity theft, to amend the Fair Credit Reporting Act, to prevent identity theft, improve resolution of consumer disputes, improve the accuracy of consumer records, make improvements in the use of, and consumer access to, credit information, and for other purposes.

Question 3: *What is identity theft?*

Answer 3: Identity theft occurs when somebody steals a person's name and other personal information for fraudulent purposes.

Question 4: *Who must comply with the Red Flags Rules?*

Answer 4: The Red Flags Rules apply to financial institutions and creditors with "covered accounts."

MORE

Question 5: *What are "covered accounts"?*

Answer 5: "Covered accounts" are those continuing financial arrangements between the University and persons owing it money that are offered or maintained primarily for personal or family needs. It also includes situations where identity theft is a reasonably foreseeable risk. A more detailed, precise definition can be found within the Red Flag Rules at: http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

---

Question 6: *The University isn't a bank or credit union, so why does it need to comply with the Red Flag Rules?*

Answer 6: FACTA requires that any entity that lends money for non-business uses, issues financial transaction cards, or is a user of credit reports to have an identity theft detection and prevention program in place. The University is required to comply with the act because it:

- handles many aspects of transactions related to loans, both on its own behalf and others (such as the Federal Government)
- issues debit cards (Blue Bucks, for example)
- uses credit reports on occasion

Question 7: *Are there separate policies for the Flint, Dearborn and Ann Arbor campuses?*

Answer 7: There is one overall policy for the three campuses. Actual implementation will vary dependent upon the particular business processes applicable to operations on the individual campuses.

MORE

Question 8: *What areas within the University are responsible for ensuring the institution complies with the Red Flag Rules?*

Answer 8: Overall responsibility for campus efforts to comply with the Red Flag Rules rests with the Office of the Associate Vice President for Finance with consultation from the Office of the Senior Vice Provost for Academic Affairs. The Hospital Executive Board provides oversight for the Health System's compliance of the Red Flag Rules.

Question 9: *When do the University's Red Flag Rules take effect?*

Answer 9: Originally scheduled for a Nov. 1, 2008 compliance date, the FTC has now delayed the enforcement date of the Red Flags Rule until Nov. 1, 2009.

Question 10: *How is the University complying with the Red Flag Rules?*

Answer 10: The University has adopted an Identity Theft Prevention Program that meets all of the criteria to carry out the intent of the Red Flag Rules and that will keep us in compliance.

Question 11: *If my department uses credit reports, how do I verify a change of address request on a covered account?*

Answer 11: When you request a credit report, you must provide the reporting agency with an address of the person whose report you requested. If there is a discrepancy between the address you provide and the address the agency has on file, the agency will send you a "Notice of Discrepancy." It then becomes your responsibility to make a reasonable inquiry into identifying a correct address, based upon information that might be available to you.

MORE

Question 12: *What constitutes a "reasonable inquiry" when attempting to confirm or locate a correct address?*

Answer 12: Using the means at your disposal to ascertain the validity of the address, up to and including contacting the owner of the covered account for which the address pertains to.

Question 13: *What if I know of a suspected identity theft situation that isn't covered in the program?*

Answer 13: First, explain the situation to your supervisor. After consultation, your supervisor may decide to call the Department of Public Safety (DPS) or may take other steps to investigate and respond. If your supervisor is not available, and someone seeking services related to a covered account has just presented you with identity documents that you strongly feel are forged, call DPS immediately.

Question 14: *What is an example of a "reasonably foreseeable risk to identity theft?"*

Answer 14: Examples of reasonably foreseeable risk to identity theft include:

- A phone request to send refund checks and a new identification card to a new address
- A loan application that's missing personal information
- A loan application that has different personal information than what is on file with U-M

These examples—and others—are considered "red flags." The Federal Trade Commission has 26 examples listed on a supplement to an Appendix to the Rules. See the following link for a complete copy of the Federal Register publication of the rules. Examples are on page 58 of the document:
http://www.ftc.gov/bcp/edu/pubs/business/alerts/alt050.shtm

MORE

Question 15: *As a staff member, is it my responsibility to notify appropriate University personnel accessing records related to the affected account holder that a Red Flag has been detected?*

Answer 15: As a University employee, it is your duty to comply with University programs and policies. You must act if you observe a violation of the Red Flag Rules. You cannot simply observe the problem and keep it to yourself.

Question 16: *What changes to information technology will occur as a result of the Red Flag implementation?*

Answer 16: No fundamental changes in information technology are needed or contemplated related to the Red Flag Rules.

Question 17: *If I'm expected to implement the Red Flag Rules, but miss a case of identity theft, will the U-M's indemnification SPG protect me if I'm sued by the victim?*

Answer 17: Acts taken by you as an employee fall under the University SPG regarding indemnification. See http://spg.umich.edu/pdf/601.09.pdf. A good faith effort by you to perform your duties, even if it turns out that something unfortunate should happen to a victim, would be indemnified by the University.

Question 18: *What are the consequences to U-M if it fails to comply with the Red Flag Rules?*

Answer 18: The University could be fined by the federal and/or state government. Enforcement is through the incorporated reference to the Fair Credit Reporting Act, namely 15 U.S.C. 1681s (a) (1). That section notes that civil fines of $2,500 per violation are established for a "knowing violation, which constitutes a pattern or practice of violations" if the fine is sought by the FCC. States have independent enforcement authority under the statute, but their standing to proceed is both limited and the potential fine is capped at $1,000. The FCC authority is limited to injunctions and, if not obeyed, the civil fine may not seek damages for losses by consumers. The states may seek damages on behalf of its residents in addition to the fine.

MORE

Question 19: *What are the responsibilities of the schools/colleges with respect to this (respect to compliance with the Red Flag Rules)?*

Answer 19: Certain aspects of the Red Flag Rules and the University's implementation program for the rules apply to a few colleges and schools that are directly executing promissory notes for their students or providing services for which payment will be made later. For the remainder of campus, these responsibilities are handled by financial personnel within central administration of the various campuses and those handling student loans through student services personnel.

Question 20: *Is a suspected identity theft case considered to be an IT security incident per SPG 601.25?*

Answer 20: It could be, dependent upon the method used to attempt to steal someone's identity. However, most identity theft situations would not likely be an IT security incident.

Question 21: *Is there a Red Flag Rules refresher training that I must take every year?*

Answer 21: No, although as with any job duties, training should be done on an "as needed" basis to insure that employees in areas covered by the Red Flag Rules are familiar with the University's Identity Theft Prevention Program.

Question 22: *What procedure will DPS use to facilitate the notification of Financial Operations of an identity theft?*

Answer 22: DPS will provide the victim with information to enable him/her to self-report the incident to Financial Operations.

MORE

Question 23: *Under what circumstances is DPS notified if an account is compromised?*

Answer 23: a) An individual (faculty, staff, retirees, and students) whose account has been compromised can always call DPS to report a potential crime. If so, then DPS would provide the victim appropriate referral information to enable self reporting.

b) Supervisor - a UM employee when presented with false documentation or evidence of identity theft on an account can call DPS for further investigation.

Question 24: *What do you mean by self-reporting?*

Answer 24: It is the individual victim's responsibility to perform the notifications to DPS and/or Financial Operations.

Question 25: *What type of complaint to DPS would trigger DPS notification to other University operations?*

Answer 25: DPS would provide the victim with information to enable him/her notification of appropriate University personnel in the event of an attempt—successful or not—to use someone's identification or account information to fraudulently obtain credit. However, it is the individual victim's responsibility to perform the notification.

###

To report a suspected incident of identity theft, or if you have questions regarding the University's Identity Theft Protection Program please call 734-615-0170.