Policy on Red Flag Rules

EFFECTIVE: November 1, 2009

LAST REVIEWED: N/A

LAST REVISED: N/A

RESPONSIBLE OFFICE: Office of Audit, Compliance and Privacy

I. **Purpose**

The purpose of this policy is to require the identification, detection and response to activity that may indicate identity theft and to comply with the FTC Red Flag Rules.

II. **Definitions**

a. "Red Flag" means a pattern, practice or specific activity that indicates the possible existence of identity theft .

III. Scope

a. *Federal requirements—Extension of Credit*

Where Penn operations involve the extension of credit, which includes allowing the deferment of payment, or arranging for the extension of credit, there must be procedures to identify, detect, and respond to Red Flags.

b. *Federal requirements—Use of consumer reports*

Where Penn operations involve the use of consumer reports, there must be procedures to respond to notices of address discrepancies received from covered consumer reporting agencies.

IV. **Extension of Credit**

In operations where Penn is involved in extending credit, which includes any operation in which Penn allows for the deferment of payment, or arranges for the extension of credit, the operational area is responsible for taking the following steps (referred to collectively as the "Identity Theft Prevention Program"):

a. Consider Red Flags in the operational area, utilizing the examples provided in FTC Red Flag Rules Appendix A, Supplement A, as a non-exhaustive checklist, and determine which Red Flags are appropriate for detection and follow-up. The examples provided in FTC Red Flag Rules Appendix A, Supplement A, are attached to this policy.
b. Develop procedures that:
    i. Based on identified applicable Red Flags:
        1. Call for the detection of such Red Flags
        2. Call for the evaluation of a detected Red Flag in a particular instance
        3. Call for, where applicable, the reporting of Red Flags for further investigation to appropriate management (see Section VI)
    ii. Require training staff involved in covered operations on such requirements
    iii. Take reasonable steps to ensure that service providers engaged to perform services in connection with extending credit, or arranging for extension of credit on behalf of Penn have reasonable policies and procedures in place to detect, prevent and mitigate risks of identity theft

iv. Require periodic reports to the Office of Audit, Compliance and Privacy regarding:
    1. Procedures of the Identity Theft Prevention Program
    2. Significant incidents of identity theft and responses taken
    3. Recommendations for material changes to the Policy on Red Flag Rules and/or its implementation

V. **Users of Consumer Reports**

When a user of consumer reports receives a notice of address discrepancy from one of the three covered consumer reporting agencies, the user must:

a. Utilize procedures to form a reasonable belief that the consumer report does relate to the consumer about whom it has requested the report. These procedures may be:
    i. Comparing the information in the consumer report, provided by the consumer reporting agency, with the information the user
        1. Obtains and uses to verify the consumer's identity
        2. Maintains in its own records
        3. Obtains from third party sources, or
    ii. Verifying information with the consumer.
b. Utilize procedures, where required, to furnish a confirmed address for the consumer to the credit reporting agency that provided the notice of address discrepancy.

VI. **Reporting Significant Risks of Identity Theft**

In all areas of Penn, instances of possible identity theft must be referred to an appropriate office for investigation.

Many cases of discrepancies in address and other information may result from simple clerical errors or information that has not been updated. In such cases, please contact the organizational unit that is responsible for maintaining the data.

In more serious cases where there is suspected inappropriate conduct or a knowing or reckless misuse of data, please contact Penn's Office of Audit, Compliance and Privacy or, particularly for concerns about criminal activity, the Penn Police.

VII. **Office of Audit, Compliance and Privacy**

Penn's Office of Audit, Compliance and Privacy is responsible for:

a. Periodically reporting to the University and Penn Medicine Trustees Committee on Audit and Compliance about the Policy on Red Flag Rules, and its implementation
b. Periodically reviewing such Policy, and
c. Providing support and assistance to Penn staff and faculty involved in implementing the Policy on Red Flag Rules

VIII. Best Practices

a. Where Penn operations are susceptible to identity theft in a manner that presents a significant risk to an individual or to the institution, but are not technically covered by the Red Flag Rules, it is a best practice to apply the steps and procedures outlined above.

IX. Effective Date

The effective date of this policy is November 1, 2009.

Attachment to Policy on Red Flag Rules:

Excerpt from Federal Trade Commission's Red Flag Rules, Appendix A, Supplement A

Alerts, Notifications or Warnings from a Consumer Reporting Agency

1. A fraud or active duty alert is included with a consumer report.

2. A consumer reporting agency provides a notice of credit freeze in response to a request for a consumer report.

3. A consumer reporting agency provides a notice of address discrepancy, as defined in §641.1(b) of this part.

4. A consumer report indicates a pattern of activity that is inconsistent with the history and usual pattern of activity of an applicant or customer, such as:

a. A recent and significant increase in the volume of inquiries;

b. An unusual number of recently established credit relationships;

c. A material change in the use of credit, especially with respect to recently established credit relationships; or

d. An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.

6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.

9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:

a. The address does not match any address in the consumer report; or

b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.

11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.

12. Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is the same as the address provided on a fraudulent application; or

b. The phone number on an application is the same as the number provided on a fraudulent application.

13. Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the financial institution or creditor. For example:

a. The address on an application is fictitious, a mail drop, or a prison; or

b. The phone number is invalid, or is associated with a pager or answering service.

14. The SSN provided is the same as that submitted by other persons opening an account or other customers.

15. The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts or by other customers.

16. The person opening the covered account or the customer fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

17. Personal identifying information provided is not consistent with personal identifying information that is on file with the financial institution or creditor.

18. For financial institutions and creditors that use challenge questions, the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

Unusual Use of, or Suspicious Activity Related to, the Covered Account

19. Shortly following the notice of a change of address for a covered account, the institution or creditor receives a request for a new, additional, or replacement card or a cell phone, or for the addition of authorized users on the account.

20. A new revolving credit account is used in a manner commonly associated with known patterns of fraud. For example:

a. The majority of available credit is used for cash advances or merchandise that is easily convertible to cash (e.g., electronics equipment or jewelry); or

b. The customer fails to make the first payment or makes an initial payment but no subsequent payments.

21. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

a. Nonpayment when there is no history of late or missed payments;

b. A material increase in the use of available credit;

c. A material change in purchasing or spending patterns;

d. A material change in electronic fund transfer patterns in connection with a deposit account; or

e. A material change in telephone call patterns in connection with a cellular phone account.

22. A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

23. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

24. The financial institution or creditor is notified that the customer is not receiving paper account statements.

25. The financial institution or creditor is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice from Customers, Victims of Identity Theft, Law Enforcement Authorities, or Other Persons Regarding Possible Identity Theft in Connection With Covered Accounts Held by the Financial Institution or Creditor

26. The financial institution or creditor is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

[72 FR 63771, Nov. 9, 2007, as amended at 74 FR 22646, May 14, 2009]