Attachment to Identity Theft Prevention Service Provider Attestation

Identify Theft Prevention Policy
Effective January 1, 2011

Identity Theft is a crime in which an individual wrongfully obtains and uses another person's personal data, usually for economic gain, in some way involving deception or fraud. This Policy attempts to reduce potential Identity Theft risks to the University and its community through 1) the implementation of an Identity Theft Prevention Program and an Identity Theft Prevention Committee, and (2) a requirement that the Identity Theft Prevention Committee identify and train certain managers and administrators of the University to identify, detect, prevent and mitigate potential Identity Theft risks. The indicators of Identity Theft are known as “Red Flags”.

Reason for the Policy

Identity theft may include various types of personal data such as an individual’s Social Security number, bank account or credit card number, telephone calling card number, medical insurance card number and other valuable identifying data. This policy sets forth the actions which must be taken by the University and by certain of its managers and administrators in order to prevent the use of personally identifiable information at Columbia University to commit Identity Theft.

Primary Guidance to Which This Policy Responds

This policy responds to the Federal Trade Commission's (“FTC”) Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003. In addition, this policy responds to all applicable state statutes pertaining to Identity Theft protection and the protection of personally identifiable information, including but not limited to, the New York State Information Security Breach and Notification Act.

Responsible University Office & Officer

The Office of the General Counsel is responsible for the maintenance of this policy, and for responding to questions regarding it. The Chief Privacy Officer and the Chief Information Security Officer are additional responsible officers.

Revision History

None to date.

Who is Governed by This Policy

This policy applies to all individuals who access, use or control personally identifiable information at Columbia University for an account, known as a “Covered Account.” A Covered Account is an account the University offers or maintains that involves or is designed to permit multiple payments or transactions, and any other account potentially posing a reasonably foreseeable risk of Identity Theft to students, patients, employees and other relevant third parties (a candidate for matriculation or for employment, for example). The risk of such harm to the individual or the University may be financial, operational, or involve compliance, reputation, or litigation risks. Those individuals may include, but are not limited to, faculty, staff, students, contractors, consultants, those working on behalf of the University and/or individuals authorized by affiliated institutions and organizations.

Who Should Know This Policy

Anyone who accesses, uses or controls personally identifiable information at Columbia University in connection with a Covered Account, as defined above, should be familiar with this policy. The Identity Theft Prevention Committee is primarily responsible for identifying and contacting individuals who must know this policy and who must undergo training.

Exclusions and Special Situations

None.

Policy Text

Columbia University acknowledges the crucial importance of its regulatory responsibilities and all reports of Identity Theft will be investigated and acted upon, up to and including the involvement of law enforcement agencies, when required. In order to meet these responsibilities, the University has established an Identity Theft Prevention Program and an Identity Theft Prevention Committee. In addition, mandatory training is being offered to certain managers and administrators of the University in order that they learn to identify, detect, prevent and mitigate potential Identity Theft risks.

The Identity Theft Prevention Program:

The program contains reasonable policies and procedures designed to:

1) Identify relevant Red Flags for new and existing Covered Accounts (both as defined below) and incorporate those Red Flags into the program;

2) Detect Red Flags incorporated into the program;

3) Respond appropriately to any Red Flags that are detected to prevent and mitigate Identity Theft;

4) Ensure the program is updated periodically to reflect changes in risks to students, patients, certain affected faculty members, and certain affected potential employees, or to reassess the soundness of the Program to protect such individuals from Identity Theft; and

5) Assist in the training of the appropriate employees in these policies and procedures in order for them to respond accordingly to any Red Flag incident.

Identity Theft Prevention Committee:

This Committee is composed of senior officers, or their designees, from various departments, such as, the Office of the Controller, the Office of the Treasurer, the Information Security Officer, the Privacy Officer, and the Human Resources Department. The Committee includes Program Managers who are responsible for identifying employees, including new employees, who handle personally identifiable information in connection with Covered Accounts (as defined below) and for oversight of their mandatory training. Program Managers are also responsible for reporting to the Program Administrator any Red Flags reported to the Program Manager by these employees.

The Identity Theft Prevention Program Administrator, also on the Prevent Committee, is an individual designated with primary responsibility for oversight of the Program, including the identification of Program Managers.

Responsibilities

The Columbia University Board of Trustees must approve the Identity Theft Prevention Program.

Responsible Executives: The Program Administrator, in connection with the Office of the General Counsel and with assistance from the Identity Theft Prevention Committee, must oversee training, compliance, and updating the Policy as necessary.

Failure to abide by this policy and/or failure to comply with the Identity Theft Prevention Program requirements may subject an individual to disciplinary action and/or sanctions

up to and including discharge or dismissal in accordance to University policy and procedures. Under the FTC Red Flag Rules, the federal government is empowered to impose civil penalties of up to $2,500 per violation, and it is possible each violation could be assessed against each Covered Account maintained by the University.

Definitions

“**Identity Theft**” is a “fraud committed or attempted using the identifying information of another person without authority.”

A “**Red Flag**” is a “pattern, practice, or specific activity that indicates the possible existence of Identity Theft.”

Examples of Red Flags include, but are not limited to:

- Alerts or notifications from consumer reporting agencies or service providers, such as fraud detection services
- Presentation of suspicious documents, such as identification documents which have been forged or altered
- Presentation of suspicious personal identifying information, such as a suspicious address change or social security number
- Presentation of suspicious personal identifying information, such as a suspicious address change or social security number
- Unusual use of or other suspicious activity relating to a Covered Account, such as identification of use of an account in a manner inconsistent with established patterns of activity on the account
- Notices from customers, victims of Identity Theft, law enforcement, or other persons regarding Identity Theft in connection with Covered Accounts held by the creditor

A “**Covered Account**” is an account the University offers or maintains that permits multiple transactions or poses a reasonably foreseeable risk of being used to promote an Identity Theft. Such an account may be identified as potentially posing a reasonably foreseeable risk of Identity Theft to students, patients, employees and other relevant third parties, including financial, operational, compliance, reputation, or litigation risks. For purposes of this program, this may include, but are not limited to:

- Certain student accounts or loans administered by the University or by third parties hired by the University to administer such accounts
- Accounts established to register patients at CUMC and Student Health Services
- Certain tenant accounts
- Certain faculty accounts or loans, and
- Certain potential employee information

"**Program Administrator**" is the individual designated with primary responsibility for oversight of the Program. After the initial Program Administrator, the subsequent Program Administrators shall be designated by the Identity Theft Committee.

"**Personally Identifiable Information**" is "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including: name, address, telephone number, social security number, date of birth, government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number, student identification number, computer's Internet Protocol address, or routing code.

Contacts

Specific inquires can be sent to the Identity Theft Prevention Committee at id_security@columbia.edu.

For general information and reports, please visit the University Compliance website at www.compliance.columbia.edu within the "Resources" section.