Coast Community College District
ADMINISTRATIVE PROCEDURE
Chapter 6
Business and Fiscal Affairs

AP 6960 IDENTITY THEFT PREVENTION

References:

15 U.S. Code Section 1681m(e), Fair and Accurate Credit Transactions Act (FACT Act or FACTA)

The risk to the District, its employees, contractors, and students from data loss and identity theft is of significant concern and can be reduced only through the combined efforts of every employee and contractor.

The District adopts these Identity Theft Prevention Procedures to help protect employees, students, clients, contractors, and the District from damages related to the loss or misuse of sensitive information. The District is complying with the regulatory requirements of the Federal Trade Commission, which issued regulations known as the "Red Flag Rules" under the Fair and Accurate Credit Transactions Act, Sections 114 and 315 (16 CFR Part 681), which amended the Fair Credit Reporting Act with the intent to reduce the risk of identity theft.

These procedures are intended to reduce the risk of identity fraud, and to minimize the potential damage to the District, and its students and clients from fraudulent activity.

These procedures:

1. Defines sensitive information;
2. Describes the physical security of data when it is printed on paper;
3. Describes the electronic security of data when stored and distributed; and
4. Places the District in compliance with state and federal law regarding identity theft protection.

These procedures will ensure the District can:

1. Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible identity theft within new or existing covered accounts;
2. Detect "red flags" when they occur in covered accounts;
3. Respond to any detected "red flags" to determine, prevent, and mitigate identity theft; and
4. Update the procedures periodically, including reviewing the accounts that are covered and the identified risks.

APPLICATION OF PROCEDURES

These procedures apply to District employees and independent contractors, including all personnel affiliated with third parties with access to sensitive information.

PROCEDURES SCOPE

1.A: Sensitive Information

1.A.1: Definition of Sensitive Information

Sensitive information includes, but is not limited to, the following items, whether stored in electronic or printed format:

1.A.1.a: Credit card information, including any of the following:
(Note that PCI compliance requirements prohibit the e-mailing of credit card information)

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address
5. CVV numbers
6. Workplace passwords providing access to such information

1.A.1.b: Tax identification numbers, including:

1. Social Security number
2. Business identification number
3. Employer identification numbers

1.A.1.c: Payroll information, including, among other information:

1. Paychecks
2. Pay stubs

1.A.1.d: Cafeteria plan check requests and associated paperwork

1.A.1.e: Medical information for any employee or student, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

1.A.1.f: Other personal information belonging to any employee, student, or contractor, as used within the scope of the covered account. Examples of which include:

1. Date of birth

2. Address
3. Phone numbers
4. Maiden name
5. Names
6. Identification number (employee, military or social security numbers)

1.A.1.g: District personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the California Public Records Act and District board policy BP 6960. If an employee is uncertain of the sensitivity of a particular piece of information, he or she should contact their supervisor. In the event that the District cannot resolve a conflict between these procedures and the California Public Records Act, District personnel should contact District Risk Services for clarification.

1.A.2: Hard Copy Distribution

Each employee and contractor performing work for the District shall comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
3. Desks, workstations, work areas, printers, and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased when not in use.
5. When documents containing sensitive information are discarded, they will be placed inside a locked shred bin or immediately shredded using a district or campus shredding device. Locked shred bins are labeled “Confidential paper shredding and recycling.”

   District records, however, may be destroyed only in accordance with State laws and regulations and consistent with District policy.

1.A.3: Electronic Distribution

Each employee and contractor performing work for the District shall comply with the following:

Sensitive information must be transmitted using only approved District e-mail. All sensitive information must be encrypted. Electronically stored data must be secured. Any sensitive information sent electronically of the type protected under these procedures, must be encrypted and password protected and only sent to approved recipients. Additionally, a statement such as this should be included in the e-mail:

"This message may contain confidential and/or proprietary information and is intended for the person or entity to whom it was originally addressed. Any use by others is strictly prohibited."

IDENTITY THEFT PREVENTION PROCEDURES

In accordance with the "Red Flag Rules", the following procedures are adopted to provide for the proper security of "covered" accounts maintained by the District

2.A: Covered accounts

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer, student and personnel account that meets the following criteria is covered by these procedures:

1. Accounts maintained for primarily personal, family, or household purposes ; or
2. Any other accounts for which there is a reasonably foreseeable risk to the consumer or to the safety or soundness of the District from identity theft, including financial, operational, compliance, reputation, or litigation risks.

2.B: Red flags

2.B.1: Any time a red flag, or a situation closely resembling a red flag, is apparent, it should be investigated for verification. The following red flags are potential indicators of fraud. Please note that this list is not all-inclusive.

1. Alerts, notifications, or warnings from a consumer reporting agency;
2. A fraud or active duty alert included with a consumer report;
3. A notice of credit freeze from a consumer reporting agency in response to a request for a consumer report; or
4. A notice of address discrepancy from a consumer reporting agency as defined in Section 334.82(b) of the Fairness and Accuracy in Credit Transactions Act.

2.B.2: Red flags also include consumer reports that indicate a pattern of activity inconsistent with the history and usual pattern of activity of an applicant or consumer, such as:

- A recent and significant increase in the volume of inquiries;
- An unusual number of recently established credit relationships;
- A material change in the use of credit, especially with respect to recently established credit relationships; or
- An account that was closed for cause or identified for abuse of account privileges by a financial institution or creditor.

2.C: Suspicious documents

2.C.1: Documents provided for identification that appear to have been altered or forged.

2.C.2: The photograph or physical description on the identification is not consistent with the appearance of the applicant or consumer presenting the identification.

2.C.3: Other information on the identification is not consistent with information provided by the person opening a new covered account or consumer presenting the identification.

2.C.4: Other information on the identification is not consistent with readily accessible information that is on file with the District, such as a signature card or a recent check.

2.C.5: An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

2.D: Suspicious personal identifying information

2.D.1: Personal identifying information provided is inconsistent when compared against external information sources used by the District. For example:

- The address does not match any address in the consumer report;
- The Social Security number (SSN) has not been issued or is listed on the Social Security Administration's Death Master File; or
- Personal identifying information provided by the consumer is not consistent with other personal identifying information provided by the consumer.

2.D.2: Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the District. For example, the address on an application is the same as the address provided on a fraudulent application.

2.D.3: Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the District.

For example:

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.

2.D.4: The SSN provided is the same as that submitted by other persons opening an account or other consumers.

2.D.5: 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 consumers or other persons opening accounts.

2.D.6: The consumer or the person opening the covered account fails to provide all required personal identifying information on an application or in response to notification that the application is incomplete.

2.D.7: Personal identifying information provided is not consistent with personal identifying information that is on file with the District.

2.D.8: When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the consumer cannot provide authenticating information.

2.E: Unusual use of, or suspicious activity related to, the covered account

2.E.1: Shortly following the notice of a change of address for a covered account, the District receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

2.E.2: A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the consumer fails to make the first payment or makes an initial payment but no subsequent payments.

2.E.3: A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material change in purchasing or credit usage patterns

2.E.4: 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).

2.E.5: Mail sent to the consumer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the consumer's covered account.

2.E.6: The District is notified that the consumer is not receiving paper account statements.

2.E.7: The District is notified of unauthorized charges related to a customer's covered account.

2.E.8: The District receives notice from victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the District.

2.E.9: The District is notified by a student or 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.

2.E.10: The discovery of a security breach by an unauthorized party relating to protected sensitive information.

RESPONDING TO "RED FLAGS"

3.A: Once potentially fraudulent activity is detected, an employee must act promptly and without unreasonable delay because timely and appropriate response can protect customers and the District from damages and loss.

3.A.1: Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

3.A.2: The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

3.B: If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the District; and
4. Notifying the actual customer that fraud has been attempted.

PERIODIC UPDATES TO PLAN

4.A: Periodically, or as required, this Procedure, and its parent Policy, will be re-evaluated to determine whether all aspects of the procedure are up-to-date and applicable in the current business environment.

4.B: Periodic reviews will include an assessment of which accounts are covered by the Policy.

4.C: As part of the review, red flags may be added, revised, replaced, or eliminated.

4.D: Actions to take in the event that fraudulent activity is discovered also may require revision to reduce damage to the District and its customers.

CAMPUS PROCEDURE ADMINISTRATION

5.A: Involvement of management

1. The Identity Theft Prevention procedures warrant the highest level of attention.
2. Operational responsibility of the procedure is delegated to the Chancellor or designee.

5.B: Staff training

1. Immediate supervisors shall conduct staff training for all employees and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information which may constitute a risk to the District or its customers.
2. The Chancellor or designee is responsible for ensuring identity theft training for all designated employees and contractors, through the employees' immediate supervisors.
3. These employees must receive periodic training in all elements of this procedures.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the procedures are made.

5.C: Oversight of service provider/contractor arrangements

1. It is the responsibility of the District to ensure that the activities of all service providers and contractors are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider or contractor that maintains its own identity theft prevention procedures, consistent with the guidance of the Red Flag Rules and validated by appropriate due diligence, may be considered to be meeting these requirements.

Ratified December 2, 2013