Town of Discovery Bay

Program Area:	Policy Name:	Policy Number:
Administrative	Identity Theft Prevention	009
Date Established:	**Date Amended:**	**Resolution:**
May 19, 2010	N/A	2010-03

I.
PURPOSE

This Identity Theft Prevention Program ("**Program**") is being implemented in accordance with the Fair and Accurate Credit Transactions Act of 2003 (P.L. 108-159) and the Federal Trade Commission's regulations thereunder (16 C.F.R., Part 681) ("**Red Flags Rule**"). The purpose of the Program is to combat identity theft by identifying risk factors for identity theft in connection with the "covered" accounts maintained by the Town of Discovery Bay Community Service District ("**Discovery Bay**"), requiring staff to be alert to "Red Flags" that may indicate identity theft, and advising staff how to handle situations where indications of identity theft have appeared.

The Program applies to all covered accounts maintained by Discovery Bay. "**Covered accounts"** include any accounts maintained primarily for personal, family, or household purposes or that involve or are designed to permit multiple payments or transactions, including utility accounts. Covered accounts also include any other accounts for which there are reasonably foreseeable risks to customers or to the safety and soundness of the Discovery Bay from identity theft. Such risks may include financial, operational, compliance, reputation, or litigation risks.

This Program does not replace or repeal any previously existing policies or programs addressing some or all of the activities that are the subject of this Program. Rather, this Program is intended to supplement any such existing policies or programs.

II.
IDENTIFYING RISK FACTORS

Discovery Bay is required under the Red Flags Rule to assess the risk of identity theft in connection with its covered accounts. As part of this risk assessment, Discovery Bay must identify all types of potentially-covered accounts that it maintains and must review the methods by which such accounts may be opened and are maintained. Discovery Bay must review these in light of all ascertainable "Red Flags" (whether listed below or otherwise) to determine what opportunities for identity theft may arise and what measures are appropriate to address them.

A. RISK ASSESSMENT

Discovery Bay presently maintains the following types of accounts which may be "covered accounts" for purposes of the Fair and Accurate Credit Transactions Act:

Water and sewer utility services accounts

The foregoing accounts may be opened in the following manner:

Service is provided based on ownership and address information obtained from Assessor's Office. Changes in service can be effectuated by phone or in person.

The foregoing accounts are accessible to the following persons in the manner described below:

Customers may obtain information by phone or in person. Discovery Bay office staff accesses customer account information through password-protected office computers.

Discovery Bay has not previously experienced identity theft issues.

Based on the foregoing, Discovery Bay determines that there is a low risk of identity theft in connection with the covered accounts it maintains. This assessment is based specifically on the lack of previous incidents involving identity theft; the nature of the service provided (i.e., associated specific real property); the small number of individuals having access to account information; and the limited personal information (names and addresses) collected by Discovery Bay.

B. "RED FLAGS" THAT MAY INDICATE IDENTITY THEFT

The following list contains a number of "Red Flags" that may indicate identity theft. When an employee becomes aware of one or more of the following situations concerning a covered account, the employee should react as discussed in Section III, below. However, please note that the following list is merely a list of examples of indicators of identity theft. Staff should exercise sound judgment and seek further verification or report to a supervisor whenever the circumstances them to believe something is wrong, whether or not those circumstances are specifically listed below.

The Federal Trade Commission has identified a number of "Red Flags" in addition to those listed below. This list omits "Red Flags" that are believed to be inapplicable to Discovery Bay (e.g., "Red Flags" which pertain to credit reports are omitted because Discovery Bay does not perform credit checks or obtain credit reports).

All employees who interact in any way with covered accounts should be alert for the following:

Suspicious Documents

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

- Photographs or physical descriptions on the identification that are inconsistent with the appearance of the applicant or customer presenting the identification.

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

- Other information on the identification that is not consistent with readily accessible information that is on file with Discovery Bay, such as an application form or a recent check.

- A request to initiate service that appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

Suspicious Personal Identifying Information

- Personal identifying information provided that is inconsistent when compared against external information sources used by Discovery Bay.

- Personal identifying information that is provided by the customer that is not consistent with other personal identifying information provided by the customer.

- Personal identifying information provided that is associated with known fraudulent activity, as indicated by internal or third-party sources used by Discovery Bay.

- Personal identifying information provided that is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by Discovery Bay.

- An identification number provided that is the same as that submitted by other persons opening an account or belonging to other customers.

- An address or telephone number provided that is the same as or similar to the address or telephone number submitted by an unusually large number of other persons opening accounts, or other customers.

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

Unusual or Suspicious Use of Covered Account

- A new account that is used in a manner commonly associated with known patterns of fraud patterns.

- A covered account that is used in a manner that is not consistent with established patterns of activity on the account.

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

- Mail sent to the customer is returned repeatedly as undeliverable although service continues to be used in connection with the customer's covered account.

- Discovery Bay is notified that the customer is not receiving paper account statements.

- Discovery Bay is notified of unauthorized charges or transactions in connection with a customer's covered account.

Notice of Identity Theft

- Discovery Bay 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.

III.
REQUIRED PROCEDURES

Potential identity thieves may be simple opportunists or skillful, determined individuals. Even exercising best efforts, it may not be possible to completely ensure security against identity theft. Nevertheless, it is every employee's duty to protect the security of Discovery Bay's information systems and to safeguard its customers' private information to the greatest extent possible. Carefully adhering to the following procedures will help to minimize opportunities for identity thieves to exploit and will help to minimize the harm they do when an individual's identity is compromised.

Accordingly, Discovery Bay requires that all staff comply with the following procedures and further requires that all third-party service providers with whom it contracts also have in place identity theft prevention programs which comply with the Fair and Accurate Credit Transactions Act.

A. PROCEDURES FOR IDENTIFYING AND PREVENTING IDENTITY THEFT

Opening New Accounts

- Staff must review any request for service for Red Flags.
- Requests for service at a particular address must be checked against ownership records and/or other available information for that address.
- In questionable circumstances, further verification may be accomplished by, e.g., contacting the record owner of the property at which service is requested.

Monitoring Existing Accounts

- All customers must be authenticated before any information concerning a covered account may be provided.
- Staff should review usage patterns and billing histories (particularly in cases where usage continues after a period of nonpayment or escalates after a period of dormancy).
- Only authorized personnel shall be permitted to access covered accounts.
- All computers through which data concerning covered accounts may be accessed must be password-protected.
- Staff shall request from customers and shall keep only those types of customer information necessary for official purposes.

B. PROCEDURES FOR RESPONDING TO SUSPECTED OR CONFIRMED IDENTITY THEFT

Where a possible indication of identity theft (i.e., one or more "Red Flags") has arisen, staff should evaluate the significance of the Red Flag and take appropriate action. Appropriate action may include, depending upon the circumstances:

- Monitoring a covered account for evidence of identity theft.
- Contacting the customer.
- Terminating service.
- Not opening a new account.
- Notifying law enforcement.
- Determining that no response is warranted under the particular circumstance.

The facts of a particular case may warrant using one or several of these options, or another response altogether. In determining a proper response, staff should consider whether any aggravating factors heighten the risk of identity theft. For example, if staff is presented with expired photo identification, an appropriate response may be to ask for satisfactory alternative identification. If, by contrast, a long-dormant account suddenly experiences heightened activity, contacting the customer directly may be appropriate. Contacting the customer would also be appropriate in instances where identity theft has been confirmed. In still another case, if a "customer" presents fraudulent identification in person, an appropriate response may be to contact law enforcement.

IV.
RESPONSIBILITY FOR IMPLEMENTING, ADMINISTERING, AND UPDATING THE PROGRAM

The General Manager is responsible for administering this Program and for keeping it up-to-date. He or she must ensure that all staff handling accounts which are subject to this Program are appropriately trained to detect possible indications of identity theft and are trained on how to respond when they encounter a "Red Flag."

The General Manager shall be primarily responsible for ensuring that when threats to the security of Discovery Bay's customers or employees arise in connection with any service that Discovery Bay provides, those threats are responded to promptly, effectively, and in a manner that best protects Discovery Bay, its customers and its employees. The General Manager is also responsible for ensuring that all aspects of this Program are complied with.

Before the close of each fiscal year, the General Manager must prepare or must require his or her staff to prepare a report on Discovery Bay's compliance with this program. The report must, at a minimum, discuss the following topics:

1. Any significant incidents involving identity theft;
2. Management's response to those incidents;
3. How effective Discovery Bay's policies and procedures are at addressing the risk of identity theft when opening new covered accounts;
4. How effective Discovery Bay's policies and procedures are at addressing the risk of identity theft concerning existing covered accounts;
5. How effective Discovery Bay's arrangements with its service providers are at preventing identity theft;
6.

7. Whether any changes should be made to those policies or procedures or to the arrangements with service providers;
8. Any other issues that bear on the risks of identity theft to Discovery Bay's customers or personnel.

V.
UPDATING THE IDENTITY THEFT PREVENTION PROGRAM

The General Manager must review the Program at least once annually to determine and adapt to any changes in risks to consumers from identity theft. In reviewing the Program, the General Manager should be alert to, among other things:

- Changes in the risk assessment set out under Section II.
- Any Red Flags that may be identified in account systems or procedures, including associated account systems or procedures.
- Evolving methods of identity theft.
- Evolving methods of detecting, preventing or mitigating identity theft.
- Changes in business arrangements, including consolidations, associations, large-scale data or personnel transfers, or changes in service provider arrangements.

VI.
CONCLUSION

Discovery Bay is committed to protecting its customers and employees and to that end requires strict adherence to the procedures set forth in this Program. However, no set of procedures can substitute for the judgment of an individual. Alertness is therefore crucial to preventing identity theft.