RED FLAG POLICY

Purpose

DTC Communications recognizes that identity theft is a continuing and growing issue that can result in harm to its customers and employees as well as the company. Pursuant to the Federal Trade Commission's (FTC) Red Flag Rules, which implements the Fair and Accurate Credit Transaction Act (the FACT Act) of 2003, DTC has enacted a Red Flag Policy to protect DTC, its' customers and employees from Identity Theft and the related damages that may result from Identity Theft. This policy establishes procedures to:

1. Identify Covered Accounts;
2. Identify the Red Flags relevant to DTC;
3. Detect Red Flags;
4. Respond appropriately to detected Red Flags;
5. Train responsible staff; and
6. Update the program and perform risk assessment.

Scope

This policy applies to all company personnel that collect and maintain personal information.

Policy

Definitions

Account: a continuing relationship established by a person with a creditor to obtain a product or service for personal, family, household or business purposes. It includes a) an extension of credit, such as the purchase of property or services involving a deferred payment, and b) a deposit account.

Covered Account: a) An account that a financial institution or creditor offers or maintains, primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, such as a credit card account, mortgage loan, automobile loan, margin account, cell phone account, utility account, checking account, or savings account; and b) Any other account that the financial institution or creditor offers or maintains for which there is a reasonably foreseeable risk to customers or to the safety and soundness of the financial institution or creditor from Identity Theft, including financial, operational, compliance, reputation, or litigation risks.

Identity Theft: fraud committed or attempted using the identifying information of another person without their knowledge or permission.

Red Flag: a pattern, practice, or specific activity that indicates the possible existence of Identity Theft.

Service Provider: a person that provides a service directly to the financial institution or creditor.

Identify Covered Amounts

Companies are responsible for determining whether they have oversight of Covered Accounts. Companies that have a Covered Account must develop and implement a written plan that identifies relevant Red Flags for their specific Covered Account.

Identify Red Flags

DTC will identify the Red Flags associated with Covered Accounts taking into consideration the types of accounts offered and maintained, the methods provided to open and access accounts, and previous experiences with identity theft.

The following are examples of Red Flags that can be potential indicators of Identity Theft:

- Alerts, notifications, or other warnings received from consumer reporting agencies or Service Providers;
- Notice of credit freeze from a consumer reporting agency in response to a request for a consumer report;
- Notice from customers, victims of Identity Theft, law enforcement authorities, or other persons regarding possible identity;
- The presentation of suspicious documents;
- The presentation of suspicious personally identifying information, such as a suspicious address change;
- The unusual use of, or other suspicious activity related to a covered account;
- Requests to mail information to addresses not on file with DTC;
- Documents presented for the purpose of personal identification are incomplete or appear to have been altered, forged or inauthentic; and
- Person is very vague about contact information or refused to provide it.

This is not an exhaustive list.

Detect Red Flags

DTC has developed and implemented the following procedures to detect Red Flags associated with opening new or accessing existing Covered Accounts:

- Monitors account transactions for possible Red Flags. Require certain identifying information such as name, date of birth, residential or business address, driver license, or other photo identification.
- Requires multi-factor identification before conducting any transaction over the phone that relates to a Covered Account.
- Requires authorization on file before releasing personal information to a third party;
- Thoroughly follows up on each billing inquiry, especially inquiries regarding services not received and/or billing errors.
- Verifies the validity of a change of address request on an existing account and provides the customer with a means to promptly report an incorrect address.

Response to Detected Red Flags

DTC makes a reasonable effort to respond appropriately to detected Red Flags in order to prevent and mitigate Identity Theft. The response should be commensurate with the degree of risk posed. Once potentially fraudulent activity is detected, an employee must act quickly as a rapid response can protect customers from damages and loss.

If Red Flags are detected, one or more of the following steps may be taken:

- monitor the Covered Accounts for evidence of identity theft;
- request additional documentation to validate identity;
- contact the consumer and verify if the activity is fraudulent;
- where appropriate, disable access or change passwords, security codes, or other security devices;
- close the Covered Account, and if needed reopen with a new account number;
- refuse to open a new Covered Account for the customer;
- determine if law enforcement should be notified; and
- determine that no response is warranted under the particular circumstances.

DTC maintains a log of Identity Theft occurrences that contains the date, description of the incident, what Red Flags were involved, and what actions were taken to avoid a similar situation from occurring in the future.

Train Responsible Staff

DTC trains responsible staff to perform the day-to-day application of the Red Flags procedures to a specific Covered Account.

Responsible staff receive training on Red Flags Identity Theft prevention and DTC's Red Flag procedures.

Program Update and Risk Assessment

DTC conducts a risk assessment periodically. The assessment considers prior experience with Identity Theft; changes in the methods of Identity Theft; changes in the detection, prevention, and mitigation of Identity Theft; the Covered Accounts offered and administered by the DTC; and the potential Red Flags that may arise with respect to the Covered Accounts. The assessment also considers any changes in risks to customers, employees and individual account holders and to the safety and soundness of DTC from Identity Theft. Documentation of the review is maintained.