

THE W.I. CLARK COMPANY IDENTITY THEFT PREVENTION PROGRAM

The W.I. Clark Co. has developed the below policy in order to comply with FACTA (Fair & Accurate Credit Transaction Act) and The Red Flag Rule and Notices of Address Discrepancy. This program will ensure the security and confidentiality of our customer's personal information and provide guidance on the protection and accessibility to this information.

The final rules require financial institutions and creditors that hold any consumer account for which there is a reasonably foreseeable risk of identity theft, to develop and implement an Identity Theft Prevention Program (Program) for combating identity theft in connection with new and existing accounts. The Program must include reasonable policies and procedures for detecting, preventing, and mitigating identity theft.¹

Finance, Sales, Accounting and Service Department employees will be responsible for recognizing and monitoring "Red Flags" that may indicate unauthorized use or theft of customer information.

This policy applies to all customer credit information that is newly obtained or currently on file.

Credit Applications: All original applications for credit requests must be provided to the Finance Department and/or Accounting department for review/approval. Copies of such documentation are not allowed to be stored in any location other than the customers account file maintained by the Finance department and/or Accounting department.

All customer information, including applications for credit, loan documentation, request for credit verification, copies of drivers' license or tax returns shall be maintained by the Finance Department and/or Accounting department. These documents will be placed in their respective files and stored in file cabinets. No customer information is to remain unsecured or accessible to other individuals when office is closed.

Disposal of Customer Information: When disposing of customer information, all documentation must be shredded, burned or pulverized before discarding.

Outside Requests for Credit References: The Finance and/or Accounting Department has the responsibility for responding to outside credit references. All requests for credit references on customers must have written authorization from the customer to release any information. This written authorization must be faxed over prior to releasing any information. Verbal verification may not be given unless customer's prior consent was provided to the Accounting and/or Finance Department.

Below is a summary of the "Red Flag" categories and examples taken from section 114 of the Fair and Accurate Credit Transactions Act of 2003, Appendix J Section IIb and Supplement A to Appendix J.

Categories of Red Flags:²

- I. Alerts, Notifications, or other warnings received from consumer reporting agencies or service providers, such as fraud detection services;**

¹ Information provided from the Federal Trade Commission website at:
<http://www.ftc.gov/opa/2007/10/redflag.shtm>

² Information provided from the Red Flag Rules website at:
http://redflagrules.net/The_Red_Flag_LIST.html

- a. A fraud or active duty alert is included with a consumer report.
- b. A consumer reporting agency provides a notice of credit-freeze in response to a request for a consumer report.
- c. A consumer reporting agency provides a notice of address discrepancy, as defined in § 334.82(b) of the interagency guidelines.
- d. A consumer report indicates a pattern of activity this is inconsistent with the history and usual pattern of the activity of an applicant or customer such as:
 - i. A recent and significant increase in the volume of inquires;
 - ii. An unusual number of recently established credit relationships;
 - iii. A material change in the use of credit, especially with respect to recently established credit relationships; or
 - iv. An account that was closed for cause of identified for abuse of account privileges by a financial institution or creditor.

II. The Presentation of Suspicious Documents

- a. Documents provided for identification appear to have been altered or forged.
- b. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
- c. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
- d. 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.
- e. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

III. Suspicious Personal Identifying Information

- a. Personal identifying information provided is inconsistent when compared against external information source used by the financial institution or creditor. For example:
 - i. The address does not match any address in the consumer report; or
 - ii. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
 - iii. 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.
- b. 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:
 - i. The address on an application is the same as the address provided on a fraudulent application; or
 - ii. The phone number is the same as the number provided on a fraudulent application.

- c. 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:
 - i. The address on an application is fictitious, a mail drop, or prison; or
 - ii. The phone number is invalid, or is associated with a pager or answering service.
- d. The SSN provided is the same as that submitted by other persons opening an account or other customers.
- e. The address or telephone number provided is the same as or similar to the account number or telephone number submitted by an unusually large number of other persons opening accounts or other customers.
- f. 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.
- g. Personal identifying information is not consistent with personal identifying information that is on file with the financial institution or creditor.

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

- a. Shortly following the notice of a change of address for a covered account, the creditor receives a request for the addition of authorized users on the account.
- b. A new revolving account is used in a manner commonly associated with known patterns of fraud. For example:
 - i. The majority of available is used for merchandise that is easily convertible to cash; or
 - ii. The customer fails to make the first payment or makes an initial payment but no subsequent payments.
- c. A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example
 - i. Nonpayment when there is no history of late or missed payments;
 - ii. A material increase in the use of available credit;
 - iii. A material change in purchasing or spending patterns;
 - iv. A material change in telephone call patterns in connection with the account.
- d. 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).
- e. Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.
- f. The financial institution or creditor is notified that the customer is not receiving paper account statements.
- g. The financial institution or creditor is notified of unauthorized charges or transactions in connection with the customer's covered account.

V. 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.

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

Response to “Red Flags”

When a possible “Red Flag” has been discovered against one of our customer’s accounts, the following appropriate mitigating responses should be taken:

- a. Monitor the affected account for evidence of identity theft,
- b. Contact the customer,
- c. Change any passwords, security codes, or other devices that permit access to the affected account.
- d. Reopen an affected account with a new account number,
- e. Decide not to open a new account,
- f. Close the account,
- g. Notify law enforcement agencies, or
- h. Determine that no response is warranted under the particular circumstances.

Program Administration

All staff will be trained as necessary for the implementation of this program.

This program shall be reviewed annually and updated periodically to reflect changes in risks to customers from identity theft, changes in methods to detect, prevent and mitigate identity theft.