Fair Credit Reporting Act Policy

Summary of Law and Regulation

The Fair Credit Reporting Act regulates the consumer credit reporting and related industries to insure that consumer information is reported in an accurate, timely, and complete manner to give individuals information when consumer reports are used to evaluate credit applications and to protect the confidentiality of information. The Fair and Accurate Credit Transaction Act (The FACT Act) amends the FCRA, establishing numerous requirements that provide protection for the victims of identity theft, provide more information to consumers about credit reports and credit scoring, limits sharing of information with affiliates, and protects consumer medical and other information

Policy

It is policy of Vizcaya Services Inc. to:

- Obtain a credit report or data on a consumer for legitimate business need only primarily in determining the consumer eligibility for:
- Credit used primarily for personal, family or household purposes;
- Employment purposes;
- Respond to fraud and activity duty alerts
- Properly dispose of consumer report information
- Provide information to victims of identity theft
- Properly handle notice of identity theft
- Respond to any notification received from identity theft, to prevent refurnishing blocked information
- Truncate the last 5 digits of a debit or credit card
- Comply with the rules regarding sharing information with affiliates
- Provide an oral, written, or electronic notice to those who receive less favorable terms in accordance with the CRA
- Comply with guidelines adopted by the Federal banking agencies, and the FTC for use when furnishing information to a Credit Reporting Agency (CRA) regarding the accuracy and integrity of the information relating to consumer that such entities furnish to CRA's
- Provide the required notice and credit score--if and when applicable
- Provide the notice regarding negative information
- Take appropriate action when Vizcaya Services Inc. receives a notice of discrepancy in the consumer's address
- Comply with the red flag guidelines

Risk Assessment

The Compliance Officer is responsible for the initial ID Theft risk assessment and ongoing updates of that assessment as needed.

Internal Controls

The Compliance Officer is responsible for assuring that appropriate written procedures and internal controls are adopted for all departments to assure compliance. The senior Management is responsible, along with the Compliance Officer, for developing, implementing and complying with appropriate controls to assure that the procedures are followed.

Training

All employees must receive training, in an appropriate format, on the basic requirements of FCRA/FACT Act.

General Procedure

When applicable, the authorized personnel will obtain a credit report for all new requests for credit upon receipt of a completed and signed application. A credit report may also be obtained for renewals or reviews of existing credit obligations and for guarantors of a credit obligation, where applicable.

Access to the Credit Reporting Agency (CRA) will be limited to authorized employees. Any employee that is not authorized to obtain a credit report and does so or any employee that obtains a credit report for any purpose other than legitimate business need will be written up for the first offense.

A credit report will not be obtained on a non-applicant spouse or any individual in connection with a business purpose loan when the consumer will not be personally liable for repayment (e.g. where the individual is merely a shareholder, officer or director of a corporation and will not guarantee or co-sign the loan)

Transactional credit information on all Vizcaya Services Inc. customers will be reported in a timely and accurate manner to the appropriate credit reporting agency. Consumer

disputes will be investigated in a timely manner by the loan operations department and the findings of that investigation reported to the appropriate credit reporting

A Statement of Adverse Action will be mailed promptly to any consumer whose loan request has been denied a loan with or approved on terms less favorable to the consumer than those for which the consumer applied. The Adverse Action Notice will be completed stating the name, address and telephone number of the consumer reporting agency that supplied the report, if appropriate. If requested by the applicant, Vizcaya Services Inc. will provide the nature of the information that Vizcaya Services Inc. relied upon to reach its decision.

ECOA allows Vizcaya Services Inc. to send one Adverse Action Notice, even when there are multiple applicants. FCRA requires that an Adverse Action Notice be sent to each co-applicant, proposed co-guarantor or similar consumer party in the particular transaction *whose credit report was used in the decision to deny*. Any questions regarding who is entitled to an Adverse Action Notice should be directed to the Compliance Officer.

A signed authorization from the customer must be received by a Vizcaya Services Inc. Employee before any request by persons or entities outside Vizcaya Services Inc. for credit information will be completed. A copy of the request for credit will be kept in a file titled “Credit Inquiries”.

IDENTITY THEFT PROCEDURE

Definition:
Financial identity theft occurs when someone uses another consumer’s personal information (name, social security number, etc) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may include opening deposit accounts with counterfeit checks, establishing credit card accounts, establishing line of credit, or gaining access to the victim’s accounts with the intent of depleting the balances.

This differs from check fraud (forged signature or forged endorsement) or an unauthorized ATM or Debit Card transaction in that it involves more than an isolated single act of fraud. Some examples of Identity Theft include:

Account Takeover

Account takeover is one of the more prevalent forms of Identity Theft. It occurs when a fraudster obtains an individual's personal information (account number and social security number is usually all it takes) , and changes the official mailing address with that individual's Company. Once accomplished, the fraudster has established a window of opportunity in which several transactions are conducted without the victim's knowledge using the victim's personal information. Notice, this involves the intent to take over the victim's identity as well as more than one isolated transaction.

It can also occur when the fraudster pays employees of various companies to steal account information from the checks that are remitted for payment. The employees will provide the name, address, bank routing number and bank account number. The fraudster will then order checks from a third party check vendor, and begin writing checks on the victims account.

Credit Take Over

Credit takeover is another form of Identity Theft that is becoming more prevalent. It occurs when a fraudster obtains an individual's personal information (social security number is usually all it takes) and establishes credit using that social security number. This may include opening credit card accounts or taking out loans without the victim's knowledge. Again, this involves the intent to take over the victim's identity as well as more than an isolated transaction.

IDENTITY THEFT INVOLVING VIZCAYA SERVICES INC.

The following procedures are to be observed when a consumer reports suspected identity theft involving Vizcaya Services Inc. or a customer account.

WRITTEN NOTIFICATION

The consumer is required to notify Vizcaya Services Inc. in writing if they suspect they are a victim of identity theft and that it involves an account or loan with Vizcaya Services Inc. . If the initial notification is made by phone, then the customer is requested to email, fax or send in writing a notice indicating that the customer did not take out the loan.

IDENTIFICATION: Request customer provide a copy of the consumer's photo identification. Attach the copy of the consumer's identification and the police report to the customer's account file.

BLOCK OR CLOSE THE ACCOUNT

If the account in question is a loan account, the appropriate steps will be taken to place a hold on the account, block the reporting of that loan to the CRA and place an alert on the account to indicate that the owner is a victim of ID Theft.

Prior to providing any information regarding the account to the consumer, It is critical that Vizcaya Services Inc. first verifies that we are dealing with the victim of identity theft rather than the perpetrator of the crime. Inform the consumer that Vizcaya Services Inc. will contact them after verifying the Police Case Number or FTC affidavit of identity theft.

Notification of Suspected Identity Theft
Guidelines for Consumer Completion

Note: Please be certain to provide all the information requested on this form. Failure to do so may cause a delay in our investigation.

1. **Name**: Please provide your ***full legal name***.

2. **Name on Account(s) if different than above:** Provide any names on valid accounts that may be different than above. For example, your legal name may be William and the name of the account would be Bill.

3. **SS#: Social Security Number**

4. **Phone Number:** The number where we may reach you during our investigation.

5. **Physical Address:** Your current ***physical*** address. P.O Boxes are not acceptable.

6. **Mailing Address:** List your mailing address if different from your physical address.

7. **Account Number(s) of suspected fraud:** Provide the account numbers associated with the suspected fraud if the account numbers are known to you.

8. **Police Case Number or FTC affidavit of identity theft:** Provide the assigned case number. We will be unable to initiate an investigation without it.

9. **Provide a detailed statement describing the questionable activity and the documents/information you are requesting from us.** You may attach additional pages as needed.

10. **Date of the application or transaction in question.** Provide the dates of the suspected activity if known.

11. **Please provide any additional information that may assist with our investigation.**

12. **Please be certain to authorize us to release information pertaining to this investigation as indicated by you.**

13. **Please sign and date the form. NOTICE that your signature MUST BE NOTARIZED.**

Mail this information to:

Vizcaya Services Inc.
8314 ½ S Kedzie Ave
Chicago, IL 60652
Attn: Compliance Officer

Be sure to enclose a NOTARIZED copy of your current driver's license or state issued photo ID. Please see the reverse side of this form for a listing of acceptable identification.

Acceptable forms of primary identification include:

- **Current US Driver's License with photo**
- Current State Issued Identification card with photo
- Current Passport
- Current Military Identification card

NOTIFICATION OF SUSPECTED IDENTITY THEFT

To be completed by the alleged victim:

PLEASE PRINT

Date: __/__/_____

1) Full Legal Name: _____

First Middle Last

2) Name on Account(s) if different than above: _____

3) SS#: _____

4) Phone Number: _____

5) Physical Address: _____
6) Mailing Address _____
_____

_____

7) Account Number(s) of suspected fraud:
_____
_____
_____
8) Please provide account information for all ***valid*** accounts with the bank:

Account #: _____
Account Type: _____

Account #: _____
Account Type: _____

Account #: _____
Account Type: _____

____
NOTE: You must provide the Police Case Number assigned to this case. Vizcaya Services Inc. will not begin an investigation without a valid case number.

9)

Police Case or FTC affidavit #_____

10)
Please provide a detailed statement describing the questioned activity and the documentation that is being requested (attach additional page(s) if needed):

11)
Date of the application or transaction in question: _____

12)
Please list any additional information you may have that will assist with our investigation.

13) I authorize Vizcaya Services Inc. to provide information relating to this case to: (check those that apply):

- Only those who have signed below.
- The following Federal, State, or local government law enforcement agency or officer:
  _____

14) By signing below, I _____, attest to the accuracy and truthfulness of the information provided above.

_____ **Notary:**

_____
Signature
My Commission Expires: _____

RED FLAG

Definitions:

Red Flag:
a pattern, practice, or specific activity that indicates the possible risk of identity theft.

Policy

It is the policy of Vizcaya Services Inc. to comply with the Fair Credit Reporting Act's ("FCRA") Identity Theft Red Flags provisions and to implement a risk-based program that detects, prevents, and mitigates the risk of identity theft in connection with both the opening of covered accounts and any existing covered accounts.

Oversight, development, implementation, and administration of this Policy and its procedures will be the responsibility of the Compliance Officer. The program and procedures will be reduced to writing and may incorporate existing policies, procedures, and processes that are designed to control any foreseeable risk to customers or to the safety and soundness of Vizcaya Services Inc..

Specifically, the board directs management to ensure that Vizcaya Services Inc. has an identity theft program that will:

- Conduct a risk assessment of all accounts that are offered and maintained to determine which accounts meet the definition of a 'covered account'. The assessment must consider the methods used to open accounts, the methods used to access accounts, and the entity's previous experience with identity theft.
- Identify "red flags" that are relevant to detecting a possible risk of identity theft to customers or to the safety and soundness of Vizcaya Services Inc.;
- Verify the identity of persons opening accounts;
- Detect red flags that management has deemed relevant in connection with the opening of an account or any existing account;
- Respond appropriately to any red flags that are detected in order to prevent and mitigate identity theft;
- Assess whether the red flags detected evidence a risk of identity theft;
- Mitigate the risk of identity theft, commensurate with the degree of risk posed;
- Train staff to implement the program; and
- Oversee service provider arrangements.

The Compliance Officer will submit a report to the board at least annually that outlines the changes in risks to customers and to the safety and soundness of the institution or as creditor relating to the identity theft program. The report will include information on:

- The effectiveness of the policies and procedures implemented by management;
- Changes in business arrangements, including mergers and acquisitions, joint ventures and service provider arrangements;
- Significant incidents involving attempted or actual identity theft and management's response to the incidents;
- Recommendations for any changes to the program

Training Employees

All employees will receive training, in an appropriate format, about identity theft. Management shall supplement that training throughout the year, as necessary, if more schemes are uncovered.

Independent Testing

Internal controls and procedures will be tested at intervals determined by Senior Management by internal and/or external auditors. Reports of these audits will be provided to management and Ownership with recommendations for corrective action.

PROVIDING INFORMATION TO VICTIMS

Definition:

Victim: a consumer whose means of identification or financial information has been used or transferred (or has alleged to have been used or transferred) without the authority of that consumer, with the intent to commit, or to aid or abet, an identity theft or a similar crime.

Procedures:

If an apparent victim of identity theft makes an appropriate request for information, the General Manager shall supply the account or loan application and the business transaction records to the apparent victim. An appropriate request must:

→Be in writing;

→Be mailed to 8314 ½ S KEDZIE AVE, CHICAGO, IL 60652 : Compliance Officer; and

→Include relevant information about any transaction alleged to be a result of identity theft to facilitate compliance with this section including, if known by the victim:

the date of the application or transaction; and

any other identifying information such as an account or transaction number

Before supplying the information to the victim, the General Manager must require the victim to provide:

→Proof of positive identification; and

→Proof of a claim of identity theft

Positive proof of identification is obtained

Proof of an identity theft claim includes:

→A copy of a police report evidencing the claim of the victim of identity theft; and

→A property completed copy of a FTC affidavit of identity theft

The General Manager will complete the **Request of Information Related to Identity Theft** and submit the form to the Security Officer for approval to block the reporting of identity theft information to a CRA or any other party. The Security Officer shall maintain the Request From and attached records for five (5) years after the date of receipt.

DISCLOSURE OF CREDIT SCORES

General Rule:

If Credit Scores are obtained in determining credit worthiness or underwriting then the following may apply:

- *The current credit score of the consumer calculated by the credit reporting agency for a purpose related to the extension of credit;
- *The range of possible credit scores under the model used
- *All of the key factors (not to exceed 4) that adversely affected the credit score of the consumer in the model used;
- *The name of the entity that provided the credit score and A separate Credit Score Notice will be provided to each applicant within 5 business days of receipt of the credit score.

NOTICE OF NEGATIVE INFORMATION

Final rule:

If any financial institution that extends credit and regularly, in the ordinary course of business furnishes information to a CRA and furnishes negative information to an agency regarding credit extended to a customer, the financial institution shall provide a notice of such furnishing of negative information, in writing, to the customer.

Definition:
Negative Information: information concerning a customer's delinquencies, late payments, insolvency, or any form of default

Model Notice:

We may report information about your account to credit bureaus. Late payments, missed payments, or other defaults on your account may be reflected in your credit report.

Or see current version of Adverse Action Notice