Fair Credit Reporting Act

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 BANK NAME to:
*Obtain a credit report on a consumer for legitimate business need only primarily in determining the consumer eligibility for:

- Credit or insurance used primarily for personal, family or household purposes;
- Employment purposes;
- Other purposes described in FCRA such as to review an account in order to determine whether the consumer continues to meet the terms of the account

*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
*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 scores
*Provide the notice regarding negative information
*Take appropriate action when the bank receives a notice of discrepancy in the consumer's address
*Comply with the red flag guidelines
*Protect medical information in the financial system

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 officer in each department 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

→ The Consumer Lending, Mortgage Lending and Indirect Lending departments will obtain a credit report for all new requests for credit upon receipt of a completed and signed application. A credit report will 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 bank staff. 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 BANK NAME 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 agency using the E-OSCAR system.

→ 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. Employees shall also check the appropriate boxes on the form to indicate the nature of the information the bank relied upon to reach its decision. All Adverse Action Notices will be signed by the loan officer making the credit decision and reviewed and initialed by a second loan officer.

→ ECOA allows the bank to send one Adverse Action Notice, even when there are multiple applicants. FCRA requires that an Adverse Action Notice be mailed 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 bank staff before any request by persons or entities outside the Bank for credit information will be completed. Only the Bank's own experience with the customer will be disclosed. A copy of the request for credit will be kept in a file title "Credit Inquiries". Each department, Deposit Operations, Loan Operations and Loan Administrations will have one of these files.

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 Take Over

Account take over 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 bank. 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 and banks 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 take over 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 HINSDALE BANK & TRUST ACCOUNT

The following procedures are to be observed when a consumer reports suspected identity theft involving a BANK NAME bank account (deposit or credit)

WRITTEN NOTIFICATION
The consumer is required to notify the bank in writing if they suspect they are victim of identity theft and that it involves an account or loan with BANK NAME. If the initial notification is made by phone and the consumer is in the area, they must be required to visit one of our branch locations to complete the "Notification of suspected Identity Theft" forms. If they are calling from outside the area, you mail or fax them a form for completion. (**NOTE: Be certain to inform the consumer that we will not begin an investigation until we receive the completed "Notification of Suspected Identity Theft form.)** Be certain to include "**consumer** guidelines for completion" in the mailing or fax.

If the consumer comes into one of our branch locations, assist them in completing the "Notification of Suspected Identity Theft" form using the guidelines in included in the "Guidelines for Consumer Completion".

I**NDENTIFICATION**: Make a copy of the consumer's photo identification.
Attach the copy of the consumer's identification and the police report to the completed Notification of Suspected Identify Theft. Forward a copy to the Security Officer.

IDENTITY THEFT – What's It All About brochure
Provide the consumer with the Identity Theft – What's It All About brochure and review the information with the consumer. Inform the consumer of their right to place a fraud alert on their credit reports (page 12 of the brochure)

BLOCK OR CLOSE THE ACCOUNT AND OPEN A NEW ACCOUNT :
If the account in question is a deposit account, close that account and open a new one for the consumer. The customer should use new PINs and passwords on the new account. Place an alert on CIF (Central File) via the officer code "999" to indicate that the owner is a victim of ID Theft. Add the information regarding the ID Theft to the Hold Transactions excel sheet (hbt/hold transactions), as a means of notifying all tellers and personal bankers of the situation. The Security Officer will determine the course of action once the investigation is complete.

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 CIF (Central File) via the officer code "999" to indicate that the owner is a victim of ID Theft.

Do not give any information regarding the account to the consumer. It is critical that the bank first verify that we are dealing with the victim of identity theft rather than the perpetrator of the crime. Inform the consumer that the bank's Security Officer will contact them after verifying the Police Case Number or FTC affidavit of identity theft.

BANK NAME
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 that 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. **Valid First National Bank Accounts:** Please provide the account numbers and account type for accounts that you have with the bank.
9. **Police Case Number or FTC affidavit of identity theft:** Provide the assigned case number. We will be unable to initiate an investigation without it.
10. **Provide a detailed statement describing the questionable activity and the documents/information you are requesting from us.** You may attach additional pages as needed.
11. **Date of the application or transaction in question.** Provide the dates of the suspected activity if known.
12. **Please provide any additional information that may assist with our investigation.**
13. **Please be certain to authorize us to release information pertaining to this investigation as indicated by you.**
14. **Please sign and date the form. NOTICE that your signature MUST BE NOTARIZED.**

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

Mail this information to:

BANK NAME
ADDRESS
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

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

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. The bank 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 the bank to provide information relating to this case to: (check those that apply):

❒ Only those who have signed below.

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

_____

❒ 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: _____

For Hinsdale Bank and Trust Co Use Only

To Be Completed by the Branch/Department Receiving the Notification

PLEASE PRINT

Received by: _____ Branch/ Department: _____ Phone Ext:_____

Date Received: _____

Verification of Identification:

Primary ID:
ID Country/State: _____ ID Type: _____
ID #: _____
Issue Date: _____ Exp. Date: _____

Send the completed form to the Security Officer with copies of the identification cards.

To Be Completed by the Security Officer

PLEASE PRINT

Date Research Completed: _____ Completed by: _____

Information provided to _____ as specified by the victim above.

Date Provided: _____

FRAUD AND ACTIVITY DUTY ALERTS

Definitions:

Fraud Alerts: a statement in the CRA file of a consumer that:

→Notifies all prospective users of a consumer report relating to a consumer that the consumer may be a victim of fraud, including identity theft; and

→Is presented in a manner that facilitates a clear and conspicuous view of the statement described in the above paragraph by any person requesting such consumer report

The FACT Act establishes three types of fraud alerts:

*Initial fraud alert –no less than 90 days - consumer asserts in good faith a suspicion of ID Theft

*Extended fraud alert – 7 year period – reported ID Theft to local police or FTC

*Active duty alert – not less than 12 months – assigned to service away from the usual duty station of the consumer

Procedures:

Upon receipt of a consumer report that contains an initial, extended or active duty alert, it is the responsibility of the personal banker or loan officer to re-verify the identity of the customer, utilizing the current CIP procedures, plus require at least one additional piece of verification. If the alert contains instructions to contact the consumer before taking any action on the request, then the personal banker or loan officer must contact the consumer in the manner specified to verify identity. No loan will be closed and funded until the identity of the applicant has been verified. All investigation information will be noted and kept in the customer file.

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 **BANK NAME** ("the bank") 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 the bank. Guidelines included in Appendix J and Supplement A of the FCRA regulation have been considered in the development of the bank's program and procedures.

Specifically, the board directs management to ensure that the bank 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 the bank;

- 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 inorder 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 least annually by internal and/or external auditors. Reports of these audits will be provided to management and the Board 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 Operations Officer 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 25 E First Street, Hinsdale, Illinois 60521 Attn: 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 Operations Officer must require the victim to provide:

→Proof of positive identification; and

→Proof of a claim of identity theft

Positive proof of identification is obtained using the current CIP procedures. 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 Operations Officer 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 identify 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.

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

REQUEST FOR INFORMATION RELATED TO IDENTITY THEFT

Person Making the Request:

Name: _____

Address: _____

_____

Proof of ID:

_____

Evidence of ID Theft:

_____

Type of Account:

_____

Action Taken:

_____

Person completing the form: _____

Supervisor: _____

Please attach records related to the identification of the requester and the proof of the ID Theft

---

REPOLLUTION

Definition: repollution is refurnishing information on an account that has been identified as information resulting from an alleged identity theft, notification from either a CRA or a consumer via an identity theft report.

Procedures:
The repollution procedures will be followed when the bank receives:

→Notice from a CRA that information the bank provided resulted from Identity Theft; or

→An Identity Theft Report from a consumer

When either above-described item is received, the Senior Loan Officer will complete a Notice of Identity Theft form and attach the information received from either the CRA or the customer. The Notice Form and attached material will be delivered to the Vice President – Loan Operations on the day of receipt. After the investigation has been completed, verification of the information, the Vice President Loan Operations will take action to block the information from reporting to a CRA or any party within 24 hours of receipt. If the account is a deposit account, generally this is accomplished by closing the suspected account and opening a new account for the customer, if appropriate.

The Vice President – Loan Operations will sign acknowledging receipt of the Notice of ID Theft and placement of the block and forward a copy to the Compliance Officer within 24 hours of placing the block.

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

NOTICE OF IDENTITY THEFT

Party Submitting the Information (CRA or Consumer):

Name: _____

Address: _____

_____

Date and time or receipt: _____

Verification of Consumer Identity:
Details of alleged ID Theft: _____

_____

Signature of the Senior Loan Officer: _____

I acknowledge receipt of this notice. The information that has been reported as resulting from identity theft:

__ Has been blocked
__ Had not been blocked for the following reason(s):

_____

Signature of VP – Loan Operations: _____

NOTICE OF ACTION TAKEN REGARDING PRICING (regulation not yet final)
General Rule:

An oral, written, or electronic notice of action taken is required when a consumer report is used in connection with an application for, or a grant, extension, or other provision of, credit on material terms that are materially less favorable than the most favorable terms available to a substantial proportion of consumer from or through that person, based in whole or in part on a consumer report.

Definitions:

Material Terms: - - - - - - -

Materially less favorable than the most favorable terms available to a substantial proportion of consumers from or through that person: - - - - -

Procedures:

(To be completed when regulation final)

RESPONSIBILITY OF FURNISHERS OF CREDIT INFORMATION

General Rule:

The Federal banking agencies, the National Credit Union Administration, and the FTC are required to:

*Establish and maintain guidelines for use by each person that furnished information to a CRA regarding the accuracy and integrity of the information relating to consumers that such entities furnish to CRAs, and update such guidelines as often as necessary; and

*Prescribe regulations requiring each person that furnishes information to a CRA to establish reasonable policies and procedures for implementing the established guidelines.

It is a prohibited practice for a person to furnish information relating to a consumer to any CRA if the person:

*Knows or has reasonable cause to believe that the information is inaccurate; or

*The person has been notified by the consumer, at the address specified by the person for such notices, that specific information is inaccurate, and the information is, in fact, inaccurate.

Definition:

Reasonable cause to believe that the information is inaccurate means having specific knowledge, *other than solely allegations by the consumer*, which would cause a reasonable person to have substantial doubts about the accuracy of the information.

Procedures:

BANK NAME will:

Provide Accurate Information to the Consumer Reporting Agencies (CRA):

*The Bank will not furnish information relating to a consumer when the Bank knows or has reasonable cause to believe that the information is incorrect.

*Upon notice and investigation of an inaccuracy, the Bank will no longer furnish that inaccurate information to the CRA.

*The Bank will promptly notify the CRA, thru E-OSCAR, of any corrections to the information being reported on a consumer

*The Bank will notify the CRA no later than 90 days after furnishing information regarding a delinquent account being placed for collection, charged to profit or loss or subject to any similar action, the date of delinquency on the account.

*The Bank will utilize E-OSCAR for notification of blocked accounts as a result of Identity Theft and will discontinue the reporting of that information.

*The Bank will act upon any notification of dispute by a consumer with the same due diligence as notifications received via E-OSCAR

Disputing Information Directly With the Furnisher

General Rule:

A consumer can dispute the accuracy of credit information either through a CRA or directly with the furnisher at the address specified for such notices.

Procedures:

A consumer who seeks to dispute directly with BANK NAME. shall provide a dispute notice to either the Loan Operations Manager . That dispute notice must:

*Be in writing
*Identifies the specific information that is being disputed;
*Explains the basis for the dispute; and
*Includes all supporting documentation required by the furnisher to substantiate the basis of the dispute

The Loan Operations Manager within 5 days, will:

*Conduct an investigation with respect to the disputed information;
*Review all relevant information provided by the consumer with the notice;
*Complete the investigation of the dispute and report the results of the investigation to the consumer before the end of a 30 day period that begins upon receipt of the notice; and
*If the investigation finds that the information reported was inaccurate, promptly notify each CRA to which the bank furnished the inaccurate information and provide the CRA any correction that is necessary to make the information accurate, using the E-OSCAR system.

The Loan Operations Manager is not required to follow the above steps if it is determined that the dispute is frivolous or irrelevant, including:

*When the consumer fails to provide sufficient information to investigate the disputed information; or
*The dispute is substantially the same as a dispute previously submitted

No later than 5 business days after making a determination that a dispute is frivolous or irrelevant, the Loan Operations Manager will provide a notice to the consumer by mail including:

*The reasons for the determination; and
*Identification of any information required to investigate the disputed information

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

DISCLOSURE OF CREDIT SCORES

General Rule:

The Lender who makes or arranges loans for closed end loan or open end line of credit for a consumer purpose that is secured by 1 to 4 units of residential real estate is required to provide to the consumer, as soon as reasonably practical, a credit score notice (model language to follow) and a consumer credit score statement including the following:

*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

Procedures:

The Notice to Home Loan Applicant will be provided to at least one applicant for a consumer purpose loan that is *secured by one-to-four unit residential real property, both open-end and closed-end loans*. The notice will be provided at the time of application for face-to-face applications and within 3 business days, for applications received through the mail, Internet or by phone.

A separate Credit Score Notice will be provided to each applicant within 5 business days of receipt of the credit score.

›The mortgage processor will be responsible for completing and mailing the notice for each mortgage loan applicant, utilizing the Calyz system.

›Consumer Lending staff will be responsible for completing and mailing the notice for each Home Equity Line of Credit and any other consumer purpose loan secured by one-to-four unit residential real property, utilizing the Appro system.

The Credit Score Notice will be included on the mortgage loan document checklist and Home Equity Line of Credit checklist. A loan cannot be closed and funded unless the Notice to Home Loan Application and the Credit Score Notice have been provided to the customer, as noted on the checklist.

BANK NAME
Fair Credit Reporting Act
Revised: 11/08

(sample)

NOTICE TO THE HOME LOAN APPLICANT

In connection with your application for a (home loan, home equity line of credit), the lender must disclose to you that score that a consumer-reporting agency distributed to users and the lender used in connection with your home, and the key factors affecting your credit scores.

The credit score is a computer-generated summary calculated at the time of the request and based on information that a consumer reporting agency or lender has on file. The scores are based on data about your credit history and payment patterns. Credit scores are important because they are used to assist the lender in determining whether you will obtain a loan. They may also be used to determine what interest rate you may be offered on the mortgage. Credit scores can change over time, depending on your conduct, how your credit history and payment patterns change, and how credit-scoring technologies change.

Because the score is based on information in your credit history, it is very important that you review the credit-related information that is being furnished to make sure it is accurate. Credit records may vary from one company to another.

If you have questions about your credit score or the credit information that is furnished to you, contact the consumer reporting agency at the address and telephone number provided with this notice, or contact the lender, if the lender developed or generated the credit score. The consumer reporting agency plays no part in the decision to take any action on the loan application and is unable to provide you with specific reasons for the decision on a loan application.

Name of CRA:	Trans Union
Address:	P O Box 2000 Chester, Pa 19022
Phone Number:	800-916-8800

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

Procedures:

BANK NAME includes the notice of negative information on the 10 day late notices produced for all loans. In any other situation other than late payments, including, but not limited to, insolvency, a separate notice is mailed to the customer prior to reporting the negative information to the CRA. This notice is also printed on the consumer application and home equity line of credit application.

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.

RECONCILING ADDRESSESS

General rule:

If a person has requested a consumer report relating to a consumer from a CRA; **AND** the request includes an address that substantially differs from the addresses in the file of the consumer; **AND** the agency provides a consumer report in response to the request, **THEN** the CRA must notify the requester of the existence of the discrepancy.

Procedures:

When a notice of address discrepancy is received from a CRA, enhanced CIP procedures will be followed by the loan processor and the correct address will be ascertained. Under the enhanced procedures, the customer's identity will be verified a second time and additional proof of identification will be obtained. The second verification will be noted in the consumer's file.

SHARING INFORMATION WITH AFFILIATES

Existing Rule in FCRA:

FCRA permits the sharing of:

→Transaction and experience information (the term is not defined) among affiliates; or
→"Other" information (beyond transaction and experience information) among affiliates, if the consumer is given notice and the opportunity to opt out of the sharing and the consumer does not elect to opt out.

New Rule in FACT Act:

The FACT Act expands affiliate rules to include new provisions governing marketing solicitations;

Any **eligibility information** received from an affiliate may not be used to make a solicitation for **marketing purposes** to a consumer about its products or services, unless:

→It is clearly and conspicuously disclosed to the consumer that the information may be communicated among affiliates for purposes or making such solicitations to the consumer; AND
→The consumer is provided an opportunity and a simple method to prohibit the making of such solicitations (opt out)

The FACT ACT excludes the sharing with the following information with an affiliate:

→Medical Information
→An Individualized list or description based on the payment transactions of a consumer for medical products or services; or
→An aggregate list of identified consumers based on payment transactions for medical products or services

Definitions:

Affiliate: any person that is related by common ownership or common corporate control with another person

Company: any corporation, limited liability company, business trust, general or limited partnership, associations or similar organization

Control of a Company:

●Ownership, control, or power to vote 25% or more of the outstanding shares of any class of voting security of the company, directly or indirectly, or acting through one or more other persons;

●Control in any manner over the election of a majority of the directors, trustees, or general partners (or individuals exercising similar functions) of the company; or

●The power to exercise, directly or indirectly, a controlling influence over the management or policies of the company

Solicitation:

Marketing initiated by a person to a particular consumer that is:

→Based on eligibility information communicated to that person by its affiliate

→Intended to encourage the consumer to purchase such products or service

.

It is the policy of BANK NAME not to share any nonpublic personal information of the Bank's existing or past customers with any affiliates.

PROTECTION OF MEDICAL INFORMATION IN THE FINANCIAL SYSTEM

General Rule:

A creditor shall not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit.

Definition:

Medical information:

Means information or data, whether oral or recorded, in any form of medium, created by or derived from a health care provider or the consumer that relates to:

→The past, present, or future physical, mental, or behavioral health or condition of an individual;
→The provision of health care to an individual; or
→The payment for the provision of health care to an individual

Does not include:

→The age or gender of a consumer,
→Demographic information about the consumer, including a consumer's residence address or e-mail address
→Any other information about a consumer that does not relate to the physical, mental, or behavioral health or condition of a consumer, including the existence or value of any insurance policy
→Information that does not identify a specific consumer.

Eligibility, or continued eligibility, for credit:
Means the consumer's qualification or fitness to receive, or continue to receive, credit, including the terms on which credit is offered. The term does not include:

→Any determination of the consumer's qualification or fitness for employment, insurance (other than a credit insurance policy), or other non-credit products or services;
→Authorizing, processing, or documenting a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or
→Maintaining or servicing the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit

Specific exceptions for obtaining and using medical information:

In general. A creditor may obtain and use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit—

→To determine whether the use of a power of attorney or legal representative that is triggered by a medical event or condition is necessary and appropriate or whether the consumer has the legal capacity to contract when a person seeks to exercise a power of attorney or act as legal representative for a consumer based on an asserted medical event or condition;

→To comply with applicable requirements of local, state, or Federal laws;

→To determine, at the consumer's request, whether the consumer qualifies for a legally permissible special credit program or credit-related assistance program that is—

(A) Designed to meet the special needs of consumers with medical conditions; and

(B) Established and administered pursuant to a written plan that—

(1) Identifies the class of persons that the program is designed to benefit; and

(2) Sets forth the procedures and standards for extending credit or providing other credit-related assistance under the program.

→ To the extent necessary for purposes of fraud prevention or detection;

→In the case of credit for the purpose of financing medical products or services, to determine and verify the medical purpose of a loan and the use of proceeds;

→Consistent with safe and sound practices, if the consumer or the consumer's legal representative specifically requests that the creditor use medical information in determining the consumer's eligibility, or continued eligibility, for credit, to accommodate the consumer's particular circumstances, and such request is documented by the creditor;

→To determine the consumer's eligibility for, the triggering of, or the reactivation of a debt cancellation contract or debt suspension agreement if a medical condition or event is a triggering event for the provision of benefits under the contract or agreement; or

→To determine the consumer's eligibility for, the triggering of, or the reactivation of a credit insurance product if a medical condition or event is a triggering event for the provision of benefits under the product.

Procedures:

BANK NAME will not ask for medical information from any consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for credit. When medical information is supplied to the bank, via a voluntary statement from the consumer or credit report BANK NAME will only use medical information to -

Determine the consumer's eligibility, or continued eligibility, for credit so long as:

→The information relates to debts, expenses, income, benefits, collateral, or the purpose of the loan, including the use of proceeds;

→We use the medical information in a manner and to an extent that is no less favorable than we would use comparable information that is not medical information in a credit transaction; and

→We do not take the consumer's physical, mental, or behavioral health, condition or history, type of treatment, or prognosis into account as part of any such determination.

→Authorize, process, or document a payment or transaction on behalf of the consumer in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit; or

→Maintain or service the consumer's account in a manner that does not involve a determination of the consumer's eligibility, or continued eligibility, for credit.