IDENTITY THEFT PROCEDURE

DEFINITION OF IDENTITY THEFT

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 lines 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 involved 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.

GENERAL GUIDELINES

A. WRITTEN NOTIFICATION

The victim's request for information **must:**

1) Be in writing [1]

2) Be mailed or delivered to the address specified by the bank; and

3) Include relevant information about any transaction alleged to be a result of identity theft that will assist the bank in providing pertinent information in a timely manner, including:

- ► If known by the victim (or readily available to the victim), the date of the application or transaction in question; and
- ► If known by the victim (or readily available to the victim), any other identifying information such as account or transaction numbers.
- ► Any other information that is identified by the manager (that is readily obtainable by the victim) that will assist in locating and providing critical information to the consumer.

4) **Be accompanied by "proof of a claim of identity theft":** XYZ BANK requires the following documentation:

- ► A copy of a police report and/or police case number evidencing the claim of the victim of identity theft; ***and***
- ► An affidavit of fact that is acceptable to XYZ BANK.[2]

[1] A sample "Notification of Identity Theft Form" has been included at the end of this document.

[2] This has been included in the "Notification of Suspected Identity Theft form.

IDENTITY THEFT INVOLVING AN XYZ BANK ACCOUNT

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

A. WRITTEN NOTIFICATION

The customer **must** notify the bank in **writing** if they suspect they are victim of identity theft and that it involves an account or loan. 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" form. If they are calling from outside the area, you may 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 the "***consumer*** guidelines for completion"[3] in the mailing.

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

B. **INDENTIFICATION:** Make a copy of the consumer's photo identification.

C. Attach the copy of the consumer's identification and the police report (if provided) to the completed Notification of Suspected Identity Theft. Forward copies to the bank's BSA Coordinator and forward the originals to the Fraud Desk Clerk in Deposit Operations Support.

D. **IDENTITY THEFT – HELP FOR VICTIMS CARD**

Provide the consumer with the Identity Theft – Help for Victims Card and review the information with them. In addition to the Identity Theft Cards, the following website may be helpful to the customer: www.consumer.gov/idtheft

E. **ALERTS/REMARKS**

Place an alert on account such as "Suspected identity theft. Verify identity and review all transactions". The Fraud Desk Clerk will determine, after reviewing details with appropriate management, whether a hard hold or block will be placed on the account(s).

F. **PASSWORD**

Using the Remark section, assign a password to the consumer's account(s). **Be certain to explain to the consumer that the bank will not discuss any account information without that password.**

1. Place both Customer Profile Remarks and Account Profile Remarks on the system. Include information: "Do not give out info without Password: xxxxxx"
2. Email the Teller Operations Manager located at the Main Banking Center (MBC) or the Teller Supervisor at the MBC. He/she will input the remarks on the First Teller system.

G. 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 Fraud Unit will contact them after verifying the Police Case Number.

H. Call the Fraud Unit Clerk x5796 to report the identity theft. In addition, e-mail the "XYZ BANKFC-Fraud Unit" with the details of the situation.

IDENTITY THEFT INVOLVING ACCOUNTS AT OTHER FINANCIAL INSTITUTIONS

When our customers suspect they are a victim of identity theft involving accounts at other financial institutions, it will not be unusual for them to contact us for guidance. It is the banks desire to assist our customers as much as possible in these situations, but they will need to resolve the situation with the alleged institutions.

---

[3] A sample copy of the consumer's guidelines has been included at the end of this document.

A. **Verification of Identity:** before discussing any information with the consumer, be certain to verify the identity of the individual to make certain we are speaking with the victim and not the fraudster.

B. Give the customer the "Identity Theft – Help for Victims Card" and review it with them. In addition to the Identity Theft Cards, this website may be helpful for customers for additional information: www.consumer.gov/idtheft

C. If the consumer has accounts at XYZ BANK, offer to assign a password to those accounts that will be verified for all future inquiries and telephone communications.

    a. Place both Customer Profile Remarks and Account Profile Remarks on the system. Include information: "Do not give out info without Password: xxxxxx"
    b. Email the Teller Operations Manager located at the Main Banking Center (MBC) or the Teller Supervisor at the MBC. He/she will input the remarks on the First Teller system.