# Members of XYZ BANKFC Fraud Unit Procedures

## General

Identity Theft is becoming more and more prevalent, and XYZ BANK has seen a number of cases reported over the past few weeks. The number of occurrences has raised concerns, and as a result, new regulations have been issued in an effort to help consumers prevent identity theft, and to assist them if they do become a victim. Banks are now required to have written procedures that cover the acceptance, investigation and resolution of suspected identity theft reports received at the bank.

## Reports of Suspected Identity Theft

Reports of suspected identity theft are forwarded to the bank's Fraud Desk Clerk located in Deposit Operations. The Fraud Desk Clerk will then e-mail the XYZ BANKFC Fraud Unit group.

## Required Actions

☐ **Deposit Operations and Loan Administration** are to conduct a review to determine if additional account relationships exist in the name of the consumer, and if so, they must determine whether these are legitimate accounts or accounts opened by the fraudster.

1. If additional account relationships are identified, steps must be taken to verify the validity of those accounts.
   - Compare the identification obtained when the account was opened to the victim's identification that was obtained and verified at the time the notification of suspected identity theft was received (on file in Deposit Ops at the Fraud Desk).
     - **Identifying Information Agrees:**
       If the identifying information agrees, and you are comfortable with the validity of the account, verify that the password selected by the victim has been assigned to the account. In addition, review the transactions/disbursement requests for the past six months to verify the actual owner of the account requested each. Any suspicious transactions are to be reported to the Fraud Desk Clerk immediately. In addition, an e-mail is to be sent to the XYZ BANKFC-Fraud Unit detailing the specifics.
     - **Identifying Information Does NOT Agree:**
       This indicates that the fraudster established the account, and additional research must be completed. Consult with management to determine the appropriate course of action. If it is determined that the account was opened by the fraudster, place a hold/block on the account to prevent additional transactions and notify the Fraud Desk clerk. In addition, send an e-mail to the XYZ BANKFC-Fraud Unit providing details of your findings.

       **Note:** If a negative report was sent to a credit reporting agency (CRA) on the account in the name of the victim (including ChexSystem) the CRA is to be notified of the current situation. They will flag the account as "Suspected Identity Theft".
2. If no additional account relationships are identified, notify the Fraud Desk Clerk of that fact.

☐ **Loan Administration:** If the initial alert was received from a credit reporting agency informing the bank that an item reported to the agency is the result of identity theft, the account must be blocked from future reporting to the credit reporting agency(s) until further notice.

☐ **All Others On the XYZ BANKFC Fraud Group E-mail List:** are to verify their respective department records (investment, trust, mortgage, safe deposit box rentals, credit cards etc.) and enter appropriate teller alerts, employee alerts, etc. If additional relationships are found, they are to be reported to the Fraud Desk immediately, and e-mail the XYZ BANKFC Fraud Group notifying them of your findings. Managers are to alert their staff members as appropriate. Telebanking employees, PBS etc. are to be alerted to the situation and instructed that all calls and/or inquiries received from the "customer" concerning the status of our investigation and/or accounts are to be forwarded to the Fraud Desk clerk.