# V. NEW ACCOUNT FRAUD

*New account fraud* is generally defined as fraud that occurs on an account within the first 90 days that it is open. It occurs when it is found that the account was opened with the intent to commit fraud. The process of establishing either a checking or a savings account may be done in person at a branch office or, depending on the institution's internal policies, over the Internet at the financial institution's website. Verification procedures vary among financial institutions, but have become more standardized since the PATRIOT Act was passed in the wake of the terrorist attacks of September 11. A primary provision of the Act is the mandate for financial institutions to establish policies and procedures to reasonably verify the identity of all parties seeking to open an account. The Act has made it more difficult to open fraudulent new accounts, but certainly not impossible. Financial institutions should be careful of following only the minimum standards of the Act, and instead should use these minimum standards as a basis for establishing an effective screening process. It is also important to keep in mind that new account fraud may occur on true-name accounts; therefore, identity verification will not prevent all new account frauds—other methods must be employed by the institution to combat fraud in these accounts.

If a perpetrator is successful in opening an account, the most effective loss prevention method is the application of deposit holds, up to the maximum allowable time under Regulation CC.

Regulation CC affords financial institutions the latitude to place extended holds on deposits to new customer accounts during the first 30 days of the relationship. Therefore, the perpetrator will generally either wait for a period of more than 30 days prior to making the first deposit or will make small deposits and withdrawals of cash during this period to establish an activity pattern and become familiar to tellers. After the initial 30 days, financial institutions cannot extend holds on deposits without meeting an exception under the Regulation, such as excessive overdrafts. By keeping the deposit amounts under the ceiling for managerial approval, the items are generally deposited with minimal or no holds on the funds. Perpetrators often choose the Friday or Saturday prior to a banking holiday to make the deposits, as it gives them a longer period to withdraw the funds before the deposited items are returned.

New account fraud begins with the perpetrator stealing the identity of an unsuspecting consumer. The criminal obtains the name, Social Security number (SSN), and date of birth of an unsuspecting citizen. This information is obtained by any of the information theft methods described in Chapter III. The targeted individual is unaware that his personal information is being used fraudulently until his bank accounts are emptied or he cannot get a loan due to poor credit from accounts in his name that he knows nothing about.

Now the perpetrators are ready to carry out the scheme. The checks deposited into the fraudulent new account are stolen and forged, counterfeited, or drawn on fraudulent accounts at other financial

institutions. As soon as the funds are available, they are withdrawn, and within a few days, the deposited items will be returned unpaid to the bank of first deposit. In this scenario, it is critical that the financial institution investigator have a thorough understanding of banking regulations because an error on the part of the payor bank is the best chance for recovering losses. Remember, the perpetrator didn't use his real name, so recovery through identification, apprehension, and prosecution is highly unlikely. The investigator will have to look for ways to use the body of banking laws and regulations to his advantage.

New account fraud continues to decline as financial institutions improve their new account screening processes. Lawmakers passed the PATRIOT Act with the expectation that it would deal a major blow to fraudulent accounts opened in fictitious names. The fallacy in this theory is that the PATRIOT Act identity requirements for opening a bank account are predicated on the belief that an "unexpired government ID" is sufficient proof of identity. Any fraud investigator will quickly tell you that counterfeiting government IDs is not a difficult task for the professional criminal. Financial institutions are required to comply with the ID verification provisions of the PATRIOT Act, but need to understand that while compliance with the Act is sufficient to satisfy the regulators, it is not sufficient to mitigate losses from new account fraud. It is imperative that financial institutions go beyond the requirements of the PATRIOT Act to ensure they verify the applicant's identity.

## Screening

There are numerous clearinghouses that allow financial institutions to verify an applicant's identity, as well as check his financial history with other financial institutions. Using this type of technology is certainly the most efficient and least offensive to the potential customer. Alternatively, the account representative can call the listed landlord, mortgagee, employer, or other contacts provided by the customer. If this method is chosen, the account representative should be sure to call numbers for these companies listed in a phone directory and not the number provided by the applicant. The financial institution's goal is to prevent fraudulent accounts from being opened, while the goal of the fraud perpetrators is to get past the new accounts desk. Professional white-collar criminals will target institutions that have weak screening procedures.

The Office of Foreign Assets Control (OFAC) is an office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy. It also establishes national security goals against targeted foreign countries, terrorists, international narcotics traffickers, and those engaged in activities related to the proliferation of weapons of mass destruction.

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities designated under programs that are not country specific—such as terrorists and narcotics

traffickers. Collectively, these are called *specially designated nationals* (SDNs). U.S. corporations and individuals are generally prohibited from dealing with SDNs.

As part of the new account screening process, financial institutions should conduct OFAC searches. These searches can be completed using an automated system or by manually checking new account holders on the OFAC website (www.ustreas.gov/ofac). The OFAC listing is updated often, and a financial institution's entire deposit and loan account subsidiary records should be compared to the OFAC listing frequently.

Bank Secrecy Act (BSA) regulations require financial institutions to implement a Customer Identification Program (CIP). The CIP must include risk-based procedures for determining the identity of each customer to the extent reasonable and practical, and must allow the financial institution to form a reasonable belief that it knows the true identity of the customer. These procedures must be based on the financial institution's assessment of relevant risks.

The CIP should contain risk-based procedures for verifying the information obtained above to the extent reasonable and practicable within a reasonable time, including:

- Describing the documents the financial institution will use to verify identity
- Verifying an individual's identity with a valid government-issued identification that evidences nationality or residence and bears a photograph or similar safeguard, such as a driver's license or passport
- Verifying the identity of corporations, partnerships, trusts, and other entities that are not individuals with documents that show the existence of the entity, such as certified articles of incorporation, a government-issued business license, a partnership agreement, or trust instrument

Non-documentary methods to verify identity include: contacting a customer; independently verifying the customer's identity through the comparison of information provided by the customer with information obtained from a consumer reporting agency, public database, or another source; checking references with other financial institutions; or obtaining a financial statement, to name a few. Non-documentary procedures must also address situations in which:

- An individual is unable to present a valid government-issued identification that bears a photograph or similar safeguard (such as minors, the elderly, or the disabled).
- The financial institution is unfamiliar with or questions the validity of the documents presented.
- The account is opened without obtaining documents.
- The customer opens the account without appearing in person.
- The financial institution is otherwise presented with circumstances that increase the risk that the institution will not be able to verify the true identity of the customer through documents.

### Getting Past the New Accounts Desk

Once the professional white-collar criminal is able to establish an account relationship with a financial institution, he has an avenue to pursue numerous fraud-related activities. It is much more complicated for a non-account holder to conduct transactions at a financial institution than for an established account holder to do so.

To circumvent the established procedures for opening a new account at an institution, professional white-collar criminals will pose as business professionals within the local community. These individuals will present the proper credentials and have the proper supporting documentation of lease agreements, licenses, work identification, and so on. Since a large majority of criminals who open fraudulent new accounts appear to be normal customers, it is up to the account representative to detect deception.

A professional white-collar criminal does not dress in a certain manner, present poor-quality identification, or tell a cover story with observable weaknesses. White-collar criminals have been known to dress as doctors, clergy, and law enforcement to establish and allow certain preset procedures to be circumvented. The goal of the individual opening the fraudulent account is to bypass the verification process and quickly establish the new account relationship.

The advent of online banking has changed the face of the new accounts "desk." Many financial institutions allow customers to open accounts online without ever meeting an employee. This practice is cost efficient for the financial institution, but it is also cost efficient for the fraud perpetrator and provides him with greater anonymity. As a result, most fraudulent new accounts are opened via the mail, telephone banking, or Internet banking. Financial institutions must rely on technology and internal control processes to identify fraudulent activity patterns and to prevent future losses.

Use of a consumer reporting system can verify the applicant's name, Social Security number, date of birth, and address. Depending on which system the financial institution uses, it can also report red flags such as mail-drop addresses, invalid phone numbers, use of multiple names or SSNs, and the financial history with other institutions. Use of third-party reporting systems is a good defense, and these same systems can be applied to remote account-opening procedures, such as those in Internet banking. If a fraudulent account is successfully opened, an early warning system that flags suspicious transactions is the best defense against losses.

### Warning Signs/Red Flags

Deception is paramount in the creation of fraudulent relationships at financial institutions. The goals of customer service programs and sales initiatives can hinder applicant screening. In an effort to attract new customers, financial institution personnel cannot place barriers of mistrust between themselves and the target customer. Each and every target customer should be treated with the highest level of respect

and credibility during the initial contact. Any sign of mistrust could direct a potential new customer to a competitor.

To provide quality customer service to potential new clients, customer service representatives need to be able to identify and detect the red flags of fraudulent identities. Very few individuals will establish a fraudulent account using their true identification and personal information; fraud perpetrators will assume the identity of someone else or simply make up an entire person. (Individuals using a true identity to open a fraudulent account would not be guilty of fraud or deception, but they could be prosecuted for theft.)

Hidden identifiers lie enveloped within every fictitious identity used to commit new account fraud. These identifiers can be detected by knowledgeable individuals. These commonalties are present within every attempted and successful new account fraud. Suspicious answers to personal questions should be mentally noted during the interview process and investigated as soon as the interview ends. The following are red flags that can be used to detect potential new account fraud. Remember, the presence of one or more red flags does not automatically mean fraud is occurring, but it does necessitate additional investigation into the information provided by the suspect account holder.

### *Verification of Social Security Number*

All three major credit bureaus (Experian, Equifax, and TransUnion) provide services to verify Social Security numbers. When an investigator inputs a potential customer's SSN in the search, the system returns the name associated with the SSN, a current and previous address, known employer, and year and state of issue. This information is developed from information the credit bureau has on file.

If the name provided by an applicant doesn't match that returned by the credit bureau search of the SSN, the application must be denied. Other warning signs include:

- The applicant is over 25 years of age and has a newly issued SSN. Since a majority of individuals enter the work force prior to age 25, a SSN should have been issued earlier.
- The applicant is over 25 years of age and has an established SSN, but the name and address information was established within the previous six months. Individuals who have a SSN issued will normally develop credit and identification information shortly after the SSN is issued. In this scenario, the SSN was issued—probably to a newborn—but has had no activity to date.
- Two different names with different addresses appear under the same SSN. Normally one of the names will have an established address and historical information, and the fictitious individual will have only recent information. The true SSN holder might reside in the original state of issue, while the fictitious holder might have an address in the state of application. In this scenario, the applicant simply used the established SSN of another person.

### *Primary Identification Issued Within the Previous 60 Days*

Professional white-collar criminals assuming the identity of a true citizen have to obtain legitimate identification within their state residence. The identification is normally obtained through the local Department of Motor Vehicles (DMV) and has a recent issue date. Unless the applicant has recently moved to the area from another state, his ID should be older than 60 days.

### *The Applicant's Home or Business Address Is Not in the Same Geographical Region as the Financial Institution*

The majority of individuals who open fraudulent accounts do so at branch offices outside of their immediate geographical location. Triangulation patterns can be drawn from the individual's listed residence, office, and the branch location.

### *The Address on the Presented Identification Is Different from the Home Address Provided*

A majority of white-collar criminals will obtain identification in the true identity of an unsuspecting individual. The victim's and the fraudster's information will be the same on formal documents; the only difference will be the photograph. To avoid documentation being forwarded to the victim's residence, the fraudster will provide a different address.

### *The Opening Deposit Is a Small Cash Deposit*

A large majority of fraudulent new accounts are opened with a cash deposit of under $500, with the normal range being between $50 to $250 dollars. The purpose of using cash is to avoid having to use true negotiable instruments to open the account. The white-collar criminal will not risk using counterfeit or forged items to open a new account. Banks usually place holds on new accounts to provide ample time for the check to clear before the new customer is allowed to draw funds against the deposits. No holds are placed on cash and fewer questions are asked of customers presenting small cash deposits.

### *Identification Cards for Non-Drivers*

State motor vehicle agencies issue identification cards that look like driver's licenses, but are only identification cards. Fraudsters are attracted to non-driver identification cards because of the ease of obtaining them.

The applicant's listed occupation should be questioned if a non-driver ID is used to open a new account. Does the individual's occupation require a driver's license? An individual in the delivery or courier business, for example, is required to have a driver's license and, therefore, should be able to provide one as identification.

### *Applicant Over 25 Years Old Without Previous Financial Institution History*

People who open new accounts are often in the process of moving and use checks from their old accounts as initial deposits. Most individuals will have a history at a financial institution because electronic banking, ATMs, direct deposit, and similar services are used by most working individuals. A red flag should be raised if an applicant is older than 25 but does not have prior banking experience.

### *Use of Mail Drop Address*

Private companies will rent mail drops to anyone for a few dollars a month and can refuse to provide the name of the individual who paid for the box. Almost any individual can rent a drop box without undergoing background verification. These establishments provide their customers with a valid street and city address and a box number at which to receive mail.

Local or online address verification directories can determine if an address is a mail delivery establishment. In addition, financial institutions can subscribe to a service that will alert the financial institution if a new account has been opened with a drop mail address. Apartment complex residents should also be verified through the building manager's office.

### *The Overly Friendly Applicant*

Many applicants will attempt to establish a quick and active rapport with the financial institution's new account person to make the application process run smoothly. The employee responsible for opening and overseeing new accounts should learn to recognize acts of attempted deception.

### Detection and Prevention Measures

To alleviate the threat of new account fraud activity, financial institutions' employees and management need to learn detection and prevention measures. A majority of institutions are reluctant to develop strict fraud prevention policies because determining the costs and benefits of prevention are almost impossible. Even if an account was opened under fraudulent means, until money is lost due to deception, there is no way of showing that the account would have lost money.

To prevent losses to new account fraud, a complete and thorough understanding of the warning signs or red flags is necessary. Procedural verification should include the following.

1. Ensure that the customer completely fills out the new account application, including complete name(s), address, employment, phone numbers, previous financial institution history, desire to open the account at your financial institution, etc.

2. Do not allow yourself to become intimidated by an individual presenting himself to be a professional (i.e., doctor or lawyer), new in town, or in a hurry. New account opening procedures should follow a strict pattern each and every time. Legitimate customers will understand procedural policies and normally allot the time necessary to establish legitimate account relationships.

3. Verify the customer's identity. Understand your state's protocols for issuing a driver's license or other documents and ensure that you are reviewing legitimate documentation.

4. Conduct a SSN verification of each SSN on new accounts. All three major credit agencies provide this service. The name of the applicant should match the name associated with the SSN. Previous or current address information can also be verified. The SSN verification will determine whether the number has already been issued, the year and state of issue, and if the SSN has been reported for death benefits.

5. Obtain a Tax Identification Number (TIN) and verify with the issuing agency that the number was issued and is legitimate. TINs, like SSNs, can be fabricated and are a sign of potential fraudulent activity.

6. For business accounts, visually inspect the business and make sure it is a going concern. Consider whether the business is consistent with the account activity.

7. Obtain a federal tax return or state certificate of incorporation for new corporate accounts to ensure the businesses are legitimate.

8. Watch the applicant as he provides personal information.
   - Is he reading his address and biographical data from his identification? He may not have had time to memorize the information on the identification.
   - Does he make eye contact during the interview? Lack of eye contact can indicate deception.
   - Are answers spontaneous or does he hesitate prior to answering or change his answers? Normal customers will have ready answers to all potential questions. Individuals assuming another's identity have to memorize the personal information and newly established geographical information.
   - Is he making an effort to be overly friendly and making excessive conversation? White-collar criminals will attempt to gain the confidence of personnel by becoming a friend. This is done in an effort to have personnel lower their guard and deviate from established policy.
   - Is he nervous and in a hurry? Individuals new to white-collar crime might not feel confident in their ability to deceive.

9. Never allow customers to take signature cards out of the financial institution for additional account signers to be added. All account signers should be present during the account opening process. Individuals opening business accounts often ask to take the signature cards so additional account signers can be added. Under fraudulent circumstances, the signature cards are never returned.

   If it is absolutely necessary for the signature card to leave the financial institution, the account should be set up to limit account access to signers present during the account opening process. Only when the signature card is returned, with notarized signatures, should additional account holders be added.

10. Call the new customer at home to inquire about the account opening process (and to verify that the home phone number is reliable). Use the phonebook to verify the customer's address and phone number.

11. Send a thank-you letter to every new customer after an account is opened. This provides a valuable customer service tool and can provide an early warning sign if the letter is returned. The thank-you letters should be marked "do not forward." Fraudsters often use a legitimate address and submit a change of address to the U.S. Post Office.

12. Photocopy all identification documents and place them in the applicant's file. The photocopying process should be explained to the new applicant as part of the institution's routine procedure. The normal white-collar criminal won't want his photograph on file.

13. Verify the applicant's employment by calling the employer (obtain the work phone number from the phonebook). Don't rely on a payroll check as employment verification; it could be counterfeited.

14. All applicants should be asked for both residence and business telephone numbers. During the employment verification process, the employer's number should be obtained from directory assistance. A professional white-collar criminal will provide phone numbers that ring at a pre-established location and are answered by other members of the fraud scheme.

15. Ask the following to all applicants: "Why do you want to open an account with us?" The truthful individual will have a legitimate reason and be quick to answer, while the fraudulent individual will not be prepared to answer.

16. Use a reference service or contact financial institutions listed on the application form to verify the customer's banking history, which might reveal behaviors that are just below the radar of suspicion.