FINANCIAL INSTITUTION FRAUD
V. NEW ACCOUNT FRAUD AND ACCOUNT TAKEOVERS

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; often, accounts are opened with the sole intent to commit fraud. Establishing either a checking or a savings account can be done in person at a branch office or, depending on the institution’s internal policies, on the company’s website. Verification procedures vary among financial institutions but have become more standardized since the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (PATRIOT Act) was passed in the wake of the terrorist attacks of September 11, 2001.

A primary provision of the PATRIOT 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 wary of following only the minimum standards of the provision, and instead use the minimum as a basis for establishing an effective screening process. In addition, new account fraud can occur on true-name accounts, meaning identity verification cannot prevent all new account frauds—other methods must be employed by the institution to combat such frauds.

If a perpetrator is successful in opening an account, the most effective loss prevention method is holding deposits up to the maximum allowable time. 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. Savvy fraudsters wait more than 30 days before making the first deposit, or they make small deposits and withdrawals in the first month to establish a pattern and become familiar to tellers. After the initial 30 days, financial institutions cannot extend holds on deposits without meeting an exception under Regulation CC, such as excessive overdrafts. 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 might begin with the perpetrator obtaining the name, Social Security number (SSN), and date of birth of an unsuspecting citizen. 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.

After stealing an identity, the perpetrator is ready to carry out the scheme. The checks deposited into the fraudulent new account are stolen and forged, counterfeit, 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
New Account Fraud and Account Takeovers

deposited items are returned unpaid to the bank of first deposit. In this scenario, it is critical that the financial institution's investigator have a thorough understanding of banking regulations because an error on the payor bank’s part is the best chance for recovering losses. Remember, the perpetrator did not 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 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 admit 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.

Office of Foreign Assets Control
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
New Account Fraud and Account Takeovers

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.

**Customer Identification Program**

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

**Video**

In the video titled “Chapter V: Customer Identification Program,” fraud investigation expert David Stewart explains some of the requirements of a CIP. Additionally, he touches upon the level to which banks protect the information they obtain through CIPs. (Go to acfevideo.vzaar.me/1188196 to view the video.)

**Non-Documentary Methods**

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 (e.g., 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 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 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.

**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 avoid placing barriers of mistrust between themselves and the target customer. Each and every target customer should be treated with the highest level of respect during the initial contact—but this does not entail ignoring warning signs.

Hidden identifiers lie enveloped within every fictitious identity, susceptible to detection by knowledgeable individuals. The following red flags should be investigated, although the presence of one or more red flags does not automatically mean fraud is occurring. In addition, suspicious answers to personal questions should be mentally noted during the interview process and investigated as soon as the interview ends.

**Verification of Social Security Number**
All three major credit bureaus (i.e., Experian, Equifax, and TransUnion) provide services to verify Social Security numbers. When an investigator inputs a potential customer's SSN to search, the system returns the name associated with the number, 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 does not match that returned by the credit bureau search of the SSN, the application must be denied. Other warning signs include:

- The applicant is 25 years of age or older and has a newly issued SSN. Since a majority of individuals enter the work force prior to age 25, a number should have been issued earlier.
- The applicant is older than 25 and has an established SSN, but the name and address information was established within the previous six months. Individuals who have a number issued will normally develop credit and identification information shortly after it 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 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.
New Account Fraud and Account Takeovers

*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, normally in the range of $50 to $250. 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-Driver*
State motor vehicle agencies issue cards that look like driver’s licenses but are only identification cards. Fraudsters are attracted to non-driver ID cards because they are easy to obtain.

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 Older than 25 Years Without Previous Financial Institution History**
People who open new accounts are often in the process of moving and using 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 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 the financial institution, and so on.
2. Do not be intimidated by an individual presenting himself as 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 the state’s protocols for issuing a driver’s license or other documents and ensure that legitimate documentation is reviewed.

4. Verify the Social Security number; all three major credit agencies provide this service. The name of the applicant should match the name associated with the number. Previous or current address information can also be verified. The verification will determine whether the number has already been issued, the year and state of issue, and if it has been reported for death benefits.

5. Obtain a Tax Identification Number (TIN) and verify it. TINs, as with Social Security numbers, 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 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 will not want his photograph on file.

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

14. All applicants should be asked for both residential 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: “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.

17. Do not issue starter checks during the initial account opening process. If the particular institution requires the issuance of starter checks, mail the checks after the verification process. If the
applicant’s information turns out to be fraudulent, this will avoid check orders being made through outside check vendors.

18. Avoid ordering checks until the verification process is complete. If the order is placed prior to the verification, the check vendor might not be able to halt the shipment if red flags are discovered during verification.

19. Check the addresses provided by the applicant against a list of known mail drops and receiving agencies. Never assume the applicant has an apartment or condo just because he provided an apartment or suite number.

20. Do not open a new account if the primary address is a PO Box. Account information and statements can be mailed to a PO Box, but a true residential address must be obtained for verification purposes.

21. Verify the applicant’s type of residence. If he claims to reside in an apartment, the name of the complex should be obtained. During the verification process, call the building manager to confirm the applicant’s residence.

22. Conduct a geographical comparison of the branch’s location, the applicant’s address, and his place of employment. Either the residence or place of employment should be near the financial institution.

23. Check the records of the bank to determine if the applicant has a previous relationship with the institution. The individual could claim to be a new applicant and have a two-year-old previous charge-off.

24. Ask an officer or a non-officer designee to review all applicants to ensure that the institution’s due diligence procedures have been performed.

Preventing fraudulent new accounts from being opened is the number one measure in lowering non-credit losses. By allowing illegitimate accounts to be opened, financial institutions provide white-collar criminals with the necessary vehicle to conduct fraudulent transactions at their institution. In addition to overdrawing the account, bogus checks can be negotiated. It is easier to prevent new fraudulent accounts from ever being opened than it is to prevent the use of counterfeit or forged negotiable instruments.
New Account Fraud and Account Takeovers

Video

In the video titled “Chapter V: New Account Fraud,” fraud investigation expert David Stewart describes the type of information customers typically need to provide when opening a new account, steps banks can take to ensure that a new customer is legitimate, and red flags of new account fraud. (Go to acfevideo.vzaar.me/1188198 to view the video.)

Account Takeovers

Account takeovers occur when a criminal perpetrator takes possession of a legitimate account holder’s bank and credit card accounts. The target of this crime is generally the debit and credit cards associated with the account. Account takeovers are less complicated than opening an entirely new account because the legitimate customer has already established the relationship and the funds in the account are already available.

Account takeovers start with the perpetrator acquiring the name and account number of a financial institution’s customer. Generally, this is the credit or debit card number because the information is typically mined from Internet traffic or stolen from retail stores by employees who then sell the information. Consumers who do not adequately secure their personal computers are easy targets of identity and financial information theft when they shop or bank online.

Once the name and card number is acquired, a letter is prepared and faxed to the financial institution asking that the address on the account be changed. If that is successful, then within a day or two the perpetrator will call the financial institution and order a replacement card, which will now be mailed to the new address. The card is then used to drain the account or make purchases before the account holder receives the next statement and becomes aware that he has been victimized. The perpetrator may also order new checks; however, given the difficulty of passing fraudulent checks, he is most likely to order a new credit or debit card.

Account takeovers are probably one of the easiest frauds for a financial institution to prevent. In account takeovers, awareness and training play a big role in prevention. For example, a financial institution might receive a request to change only the address for a customer’s debit card or credit card account. Most customers do not change just their debit or credit card account without changing their master account as well. Furthermore, these address changes are generally requests to change the address to a major U.S. metropolitan area, such as New York, Miami, Los Angeles, or Chicago. Typically, a financial institution customer who lives in one part of the country would not request an address change for only their debit or credit card to one of these locations and continue to receive their master account statements at their local address.
If the employees responsible for making account maintenance changes were to contact the account holder or verify the signature against financial institution records for changes requested on debit or credit cards, a majority of account takeover fraud could be prevented. If the request makes it past the account maintenance clerk, the financial institution has yet another means of stopping these losses. By generating a daily report of check orders and credit or debit card requests made within two to three days of address change requests, financial institutions can identify these changes as fraudulent before the cards are mailed out. Another simple means of identifying fraudulent address changes designed to takeover an account is to set up a “hot file” of locations where this activity is common, and have the IT department run all address changes against the hot file each night. A report can be produced for investigators to review the following day for any address changes to these locations.

Account takeovers also occur when account balances are not timely placed into probate or properly closed at the time of death of one of the authorized signers. These funds are an easy target since the account holder is deceased and family members might be unaware that the funds exist. Oftentimes, the account becomes dormant and funds are then transferred or a check is written to close the account. The fraudster will often change the mailing address of the account several months prior to closing the account. This type of fraud is often perpetrated by an insider or an employee of the bank.
New Account Fraud and Account Takeovers

Review Questions

1. Which of the following is the first step in new account fraud?
   A. Negotiating the check
   B. Stealing or creating the identity
   C. Opening the new account
   D. None of the above

2. When verifying a Social Security number (SSN), red flags of a fraudulent SSN include:
   A. The applicant is older than 25 years and has a newly issued SSN
   B. The applicant is older than 25 years with an established SSN, but the name and address
      information was established within the previous six months
   C. Two different names with different addresses appear under the same SSN
   D. All of the above

3. For which of the following reasons is the typical fraudulent new account opened with a small cash
   deposit?
   A. Cash deposits are encouraged by most financial institutions
   B. The account opener can avoid having to establish an account where the deposit item will clear
   C. Cash offers additional security for financial institution personnel on the newly opened account
   D. None of the above

4. Which law, passed in 2001, established minimum identification requirements for opening a new
   account?
   A. Bank Secrecy Act
   B. Regulation CC
   C. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and
      Obstruct Terrorism Act (PATRIOT Act)
   D. None of the above

5. Which of the following affords financial institutions the latitude to place extended holds on deposits
   to new customer accounts during the first 30 days of the banking relationship?
   A. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and
      Obstruct Terrorism Act (PATRIOT Act)
   B. Bank Secrecy Act
   C. Regulation CC
   D. Customer Identification Program
6. A verification of the applicant’s Social Security number (SSN) (non-credit report) will provide all of the following EXCEPT:
   A. Any reported names associated with the SSN
   B. Address information
   C. A credit score for cross-selling purposes
   D. Year and state of SSN issue

7. If the fraudulent address has been successfully changed, the perpetrator will MOST likely:
   A. Order new checks.
   B. Order a debit or credit card.
   C. Open another account.
   D. Apply for a loan.