AL 2001–4

OCC ADVISORY LETTER

Comptroller of the Currency
Administrator of National Banks

Subject: Identity Theft and Pretext Calling

TO: Chief Executive Officers of All National Banks, Department and Division Heads, and All Examining Personnel

I. PURPOSE

This advisory letter informs national banks about two areas of consumer bank fraud—identity theft and pretext calling—and advises them about measures to prevent and detect these types of fraud. The Gramm–Leach–Bliley Act (GLBA), enacted in 1999, directs the federal banking agencies (the Agencies) to ensure that banks have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect fraudulent access to such information.[1] The Agencies recently adopted guidelines for the safeguarding of customer information by financial institutions.[2] The advisory letter supplements those guidelines by focusing on the protection of customer information specifically against identity theft and pretext calling.

Identity theft is the fraudulent use of an individual's personal identifying information. Often, identity thieves will use another individual's personal information such as a social security number, mother's maiden name, date of birth, or account number to fraudulently open new credit card accounts, charge existing credit card accounts, write checks, open bank accounts or obtain new loans. They may obtain this information through a number of means, including

- Stealing wallets that contain personal identification information and credit cards,
- Stealing financial institution statements from the mail,
- Diverting mail from its intended recipients by submitting a change of address form,
- Rummaging through trash for personal data,

[1] 15 USC 6825. GLBA also contains specific prohibitions against obtaining customer information from a financial institution by false pretenses. *Id.* at 6821.

[2] *See* Interagency Guidelines for Establishing Standards for Safeguarding Customer Information, 66 *Fed. Reg.* 8616 (February 1, 2001). The OCC's standards are codified at 12 CFR Part 30, App. B (hereinafter, referred to as the "Guidelines for Safeguarding Customer Information").

- Stealing personal identification information from workplace records, or

- Intercepting or otherwise obtaining information transmitted electronically.

Pretext calling is a fraudulent means of obtaining an individual's personal information. Pretext callers may contact financial institution employees, posing as their customers, in order to access customers' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators for use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information for use in creating fraudulent accounts.

This advisory letter provides background information on identity theft and pretext calling and informs banks about: (1) relevant federal laws; (2) measures to take to reduce their risk of loss and protect their customers against these types of fraud; (3) how to report to law enforcement known or suspected federal criminal violations related to these types of fraud; and (4) the importance of consumer education to prevent fraud and assist individuals who have been victims of pretext calling and identity theft.[3]

II. BACKGROUND

According to the Federal Bureau of Investigation, identity theft is one of the fastest growing white-collar crimes in the nation.[4] More than 500,000 consumers are victimized each year by identity theft. This growing crime has a devastating effect on financial institution customers and a detrimental impact on the banks.[5] Four of the top five consumer complaints regarding identity theft involve financial services—new credit card accounts opened, existing credit card accounts used, new deposit accounts opened, and newly obtained loans.[6] Banks absorb much of the

[3]At the end of the advisory letter is an appendix that lists other OCC guidance regarding information security.

[4]Reasons cited for this increase in identity theft include the increased availability of personal information in the marketplace, the ability of identity thieves to use this information to, for instance, apply for credit under cover of anonymity afforded by remote channels, and the nearly instantaneous and ready availability of credit. *See, e.g.,* Testimony of the United States Secret Service to the House Committee on Banking and Financial Services, September 13, 2000.

[5]For example, the American Bankers Association (ABA) 1998 Check Fraud Survey found that $3 out of every $4 lost by a community bank to check fraud was due to some form of identity theft. In its 2000 Check Fraud Survey, the ABA found that *attempted* check fraud doubled in the past two years, exceeding $2.2 billion dollars. The survey further indicated that one-third of fraud cases and fraud losses were due to forgery.

[6]On November 1, 1999, the Federal Trade Commission (FTC) established a toll-free telephone hotline, 1-877-ID-THEFT (438-4338), for consumers to report identity theft and seek counseling. Information from complainants is stored in a central database and used as an aid in law enforcement and prevention. In testimony delivered on September 13, 2000, at a hearing on identity theft held by the House of Representatives Committee on Banking and Financial Services, the FTC reported that its identity theft hotline received over 1000 calls a week in July and August 2000. More recent public statements by FTC officials indicate that the number of calls to the hotline have more than doubled since then, to over 2000 calls a week. *See, e.g.,* Statement of Jodie Bernstein, director of the FTC's Bureau of Consumer Protection, to the President's Information Technology Advisory

economic losses from bank fraud associated with the theft of their customers' identities. Individuals who become victims of identity theft also pay, at a minimum, out-of-pocket expenses to clear their names and may spend numerous hours trying to rectify their credit records.[7]

Identity theft may go undetected for months and even years. Victims of identity theft may not realize that someone has stolen their identity until they are denied credit or until a creditor attempts to collect an unpaid bill.

Pretext calling is also difficult to detect. While information brokers and private investigators routinely advertise on the Internet and elsewhere their ability to locate and provide specific information about individual bank accounts, banks and their customers are likely to be unaware that they have been the victims of pretexting (*i.e.,* the use of some form of pretext to obtain customer information). Unless the pretexting ultimately leads to identity theft, it may go undetected altogether.

III. SUMMARY OF RELEVANT FEDERAL LAWS

Identity theft—In 1998, Congress passed the Identity Theft and Assumption Deterrence Act (18 USC 1028) (the Act). The Act makes it a crime to knowingly use, without lawful authority, a means of identification of another person with the intent to commit a crime, among other things. The unauthorized use of another individual's name, social security number, or date of birth to apply for a credit card is punishable by fine or imprisonment under this Act. The Act also requires the Federal Trade Commission (FTC) to establish a central complaint system to receive

---

Committee, February 7, 2001. Information in the FTC database collected from hotline calls for the year 2000 indicate the most common forms of identity theft reported to the FTC include:

- *Credit card fraud*—Fifty percent of complainants reported that a credit card account had been opened in their name, or an identity thief had taken over their existing account. Seventy-one percent of these complaints involved the establishment of a new account; twenty-five percent involved the takeover of an existing account. (Roughly four-and-a-half percent of complaints in this category were unspecified.)

- *Checking or savings account fraud*—Sixteen percent of complainants reported a savings or checking account had been opened in their name or fraudulent checks had been written on existing accounts. Forty-nine percent of these complaints involved using unauthorized checks; twenty-seven percent involved establishing new checking accounts; seventeen percent involved unauthorized electronic fund transfers. (About seven percent of the complaints in this category were unspecified).

- *Loan fraud*—Nine-and-a-half percent of complainants reported the identity thief had obtained a loan in their name.

See FTC Web site at www.consumer.gov/idtheft/. Click on FTC workshop and then on report charts.

[7] For example, under Regulation Z, in instances involving identity theft, a consumer could incur liability for the unauthorized use of the consumer's credit card account up to $50. Under Regulation E, a consumer's liability for unauthorized electronic fund transfers involving his or her account varies depending upon the precise circumstances of the unauthorized use and the consumer's timeliness in reporting unauthorized transactions or the loss or theft of an access card, number, or other device.

and refer identity theft complaints to appropriate entities, including law enforcement agencies and national credit bureaus.

Schemes to commit identity theft may also involve violations of other federal statutes such as the prohibition against fraudulent tax refund claims (18 USC 287), credit card fraud (18 USC 1029), computer fraud (18 USC 1030), mail fraud (18 USC 1341), wire fraud (18 USC 1343), or bank fraud (18 USC 1344). A number of states also have passed laws related to identity theft.

Pretext calling—The GLBA prohibits the making of false or fraudulent statements or representations to an officer, employee, or agent of a financial institution, or to a customer of a financial institution, to obtain customer information (15 USC 6821). The GLBA also prohibits anyone from requesting a person to obtain customer information of a financial institution, knowing that the person will use fraudulent methods to obtain information from the institution. Section 523 of the GLBA (15 USC 6823) imposes criminal penalties for knowing and intentional violations of these provisions.

While this statute is generally aimed at persons who victimize banks and their customers by attempting to obtain customer information through pretexting, banks could themselves be in violation of this statute if they use the services of any person who obtains customer information in violation of the statute. Although the statute maintains that an institution must "know" that the person will use artifice to obtain customer information, safe and sound banking practices dictate that a bank exercise reasonable diligence in selecting a third party to gather customer information. In this regard, banks should familiarize themselves with the methods used by third parties to collect customer information on their behalf. Banks should not the use the services of anyone the bank suspects may be engaging in pretexting to obtain customer information.

Security standards—Section 501(b) of the GLBA (15 USC 6801(b)) requires the Agencies to establish appropriate standards for banks relating to the administrative, technical, and physical safeguards of customer information. Banks are expected to take appropriate measures in accordance with the Guidelines for Safeguarding Customer Information to protect customer information against identity theft and pretext calling.

IV. MEASURES TO PREVENT IDENTITY THEFT AND PRETEXT CALLING

A. Identity theft

Identity thieves use a number of methods to obtain financial services in the name of another individual. For instance, an identity thief may request that a bank change the address on an existing credit card account, thereby diverting billing statements from the true account holder. Alternatively, an identity thief may order new checks on an existing account and have them sent to a mail drop, rather than the true account holder's address. An identity thief may use the personal information of another individual to apply for a new checking or credit card account.

Banks should employ a variety of methods to safeguard customer information and reduce the risk of loss from identity theft, including (1) verifying personal information to establish the identity

of individuals applying for financial products, (2) establishing adequate procedures to detect possible fraud in new accounts, (3) verifying the legitimacy of change of address requests on existing accounts, and (4) maintaining adequate security standards.

1. Verification procedures for new accounts

To reduce the risk of fraudulent applications, banks should establish verification procedures to ensure the accuracy and veracity of application information. In conjunction with their existing account opening procedures, banks should consider how best to independently verify information provided on account applications to detect incidents of identity theft. Verification of personal information may be accomplished in a number of ways. Some alternatives to consider include: (a) *positive verification* to ensure material information provided by an applicant is accurate; (b) *logical verification;* and (c) *negative verification* to ensure information provided has not previously been associated with fraudulent activity.[8]

a. Positive verification entails consulting third-party sources to assess the veracity of information submitted by a consumer. For example, an identity thief may provide the true name of an individual and a correct phone number, but an erroneous address. An institution could detect this discrepancy simply by checking a telephone directory. Under appropriate circumstances, a bank may obtain an individual's consumer report that would permit more detailed verification. Banks should consider calling a customer to confirm that the individual has opened a credit card or checking account, using a telephone number that has been verified independently. A phone call to a customer may alert an individual that his or her identity has been stolen. Additionally, a bank could contact an applicant's employer. An identity thief may provide the name of a legitimate employer, but may not provide the correct telephone number. A bank should attempt to contact an employer using an independently verified telephone number. Contacting an employer may expose a fraudulent application.

b. *Logical verification* entails assessing the consistency of information presented in an application. Such steps may reveal inconsistencies in the information provided by an applicant. For instance, a bank could verify if the zip code and telephone area code provided on the application cover the same geographical area. Products currently available from service providers can assist banks in verifying logical zip and area codes.

c. *Negative verification* entails ensuring that information provided on an application has not previously been associated with fraudulent activity.

2. Other new account procedures

Consumer reports can be an important source for preventing fraud. When processing an application for a new account, a bank may rely on a consumer report from a consumer reporting

[8]Some databases used for verification purposes may be provided by consumer reporting agencies and their use may raise issues under the Fair Credit Reporting Act.

agency. A consumer report of a victim of identity theft may be issued with a fraud alert.[9] When a bank has an automated system for credit approval, these systems should be designed to identify fraud alerts. Banks should not process an application when there is an existing fraud alert without contacting the individual in accordance with instructions that usually accompany a fraud alert *(i.e.,* a victim's statement), or otherwise employing additional steps to verify the individual's identity. The bank should have procedures in place to share a fraud alert across its various lines of business.

Consumer reports also may be a source for detecting fraud. Signs of possible fraudulent activity that may appear on consumer reports include late payments on a consumer's accounts in the absence of a previous history of late payments, numerous credit inquiries in a short period of time, higher-than-usual monthly credit balances, and a recent change of address in conjunction with other signs.

Finally, when an applicant fails to provide all requested information on an application, a bank should not process the incomplete application without further explanation.

3. Verifying change of address requests

A change of address request on an existing account may be a sign of fraudulent activity. A bank should verify the customer information before executing an address change and send a confirmation of the address change to both the new address and the address of record. If an institution gets a request for a new credit card or new checks in conjunction with a change of address notification, the bank should verify the request with the customer within a reasonable period of time after receiving the request.

4. Security standards

The Guidelines for Safeguarding Customer Information require banks to implement a comprehensive information security program that includes appropriate administrative, technical, and physical safeguards for customer information. Information security programs must be designed to ensure the security and confidentiality of customer information, protect against anticipated threats or hazards to the security or integrity of the information, and protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to customers.

Banks should take steps to secure the transmission and storage of electronic information to prevent identity thieves from gaining access to such information. This may include the use of encryption, firewalls, and other electronic data security systems and preventative measures. Identity thieves may also seek access to information that an institution discards. For instance, identity thieves may rummage through trash to collect customer information (dumpster diving). A bank should implement appropriate measures to restrict access to its customer records, such as

[9] A fraud alert is a statement that accompanies an individual's consumer report informing creditors that an individual's account has been the subject of fraud. Each of the major credit bureaus will voluntarily place a fraud alert on a consumer report upon request.

by shredding documents, to protect against dumpster diving and other forms of unauthorized access.

Banks and their service providers should implement appropriate controls and procedures to limit access to customer records. Because insiders may be identity thieves a bank should consider conducting background checks for its employees, in accordance with applicable law. Where indicated by its risk assessment, a bank should also monitor its service providers to confirm that they have implemented appropriate measures to limit access to customer records.[10]

B. Pretext calling

Pretext callers use pieces of personal information to impersonate an account holder in order to gain access to that individual's account information. Armed with personal information, such as an individual's name, address, and social security number, a pretext caller may try to convince a bank's employee to provide confidential account information. While it may be difficult to spot, there are measures banks can take to reduce the incidence of pretext calling, such as limiting the circumstances under which customer information may be disclosed by telephone.[11]

The Guidelines for Safeguarding Customer Information require banks to establish written policies and procedures to control risks to customer information, and consider access controls on customer information as part of these policies and procedures. Banks should take appropriate precautions against the disclosure of customer information to unauthorized individuals such as (1) limiting the circumstances under which employees may disclose customer information over the telephone, (2) training employees to recognize and report fraudulent attempts to obtain customer information, and (3) testing to determine the effectiveness of controls designed to thwart pretext callers.

1. Limiting telephone disclosures

There are a number of ways in which banks may limit access to customer information. One way is to permit employees to release information over the telephone only if the individual requesting the information provides a proper authorization code.[12] The code should be different than other commonly used numbers or identifiers, such as social security numbers, savings, checking, loan, or other financial account numbers, or the maiden name of the customer's mother. The authorization code should be unique to, and capable of being changed readily by, the authorized

[10] For additional information on managing relationships with third-party service providers, *see* FFIEC guidance on technology outsourcing, "Risk Management of Outsourced Technology Services," (November 28, 2000).

[11] A bank should consider appropriate procedures and limits for disclosing information through any communication channel (*e.g.,* e-mail or wireless devices) that the institution uses. As the use and acceptance of e-mail, Internet banking, and electronic account statements increase, banks should develop procedures to verify the identity of the sender of a message. In many cases e-mail may not be an appropriate channel to communicate certain types of account information. E-mail can be easily forged, hijacked, or read by people other than the intended recipient. Additionally, a forger may be difficult to trace particularly if the message is relayed through intermediate mail servers.

[12] *See, e.g.,* OCC Advisory Letter 98-11 (August 20, 1998).

account holder. To be most effective, the authorization code should be used in conjunction with other customer and account identifiers.

Another means of preventing unauthorized disclosures of customer information is to use a caller identification system (*i.e.,* CallerID™). If the telephone number displayed differs from that in the customer's account records, it may be an indication that the request is not legitimate and the employee should not disclose the requested account information without taking additional steps to verify that the true customer is making the request. In the absence of a caller identification system, banks could require employees who receive calls for account information to ask the caller for the number from which he or she is calling, or for a call-back number. If the individual refuses to provide the number, or it doesn't match the information in the customer's records, the employee should not disclose the information without additional measures to verify that the caller is the true customer.[13]

2. Employee training

Banks should train staff to recognize unauthorized or fraudulent attempts to obtain customer information. In addition to an employee's inability to match a caller's telephone number with that on file, there may be other indicators of a pretext call. For instance, a caller who cannot provide all relevant information requested, or a caller who is abusive, or who tries to distract the employee, may be a pretext caller. Employees should be trained to recognize such devices and, under such circumstances, protect customer information through appropriate measures, such as by taking additional steps to verify that the caller is a bona fide customer.

Employees should be trained to implement the bank's written policies and procedures governing the disclosure of customer information, and should be informed not to deviate from them. Moreover, employees must know to whom and how to report suspicious activity that may be a pretext call. Banks may have a fraud department or contact to whom the employee reports suspicious activities, or may establish another means for reporting possible fraud. Known or suspected federal criminal violations should be reported to law enforcement in accordance with the procedures discussed below.

3. Testing

Banks should test the key controls and procedures of their information security systems and consider using independent staff or third parties to conduct unscheduled pretext phone calls to various departments to evaluate the institution's susceptibility to unauthorized disclosures of customer information. Any weaknesses should be addressed through enhanced training, procedures, or controls, or a combination of these elements.

---

[13] There may be other circumstances in which a caller is seeking access to customer account information, such as a merchant attempting to verify whether the bank's customer has sufficient funds to cover a check. Banks should not permit their employees to provide a customer's account information without taking steps to verify the identity of the caller. For instance, banks could direct their employees to request a call back number to verify the merchant's identity. Additionally, where a bank uses an automated telephone response system to verify funds availability, the system should be password protected.

V. REPORTING SUSPECTED IDENTITY THEFT AND PRETEXT CALLING

OCC regulations currently require banks to report all known or suspected criminal violations to law enforcement and the OCC by the use of the Suspicious Activity Report ("SAR").

Criminal activity related to identity theft or pretext calling has historically manifested itself as credit or debit card fraud, loan or mortgage fraud, or false statements to the bank, among other things. Presumably, banks have been reporting such known or suspected criminal violations through the use of the SARs, in accordance with existing regulations.

As a means of better identifying and tracking known or suspected criminal violations related to identity theft and pretext calling, a bank should, in addition to reporting the underlying fraud (such as credit card or loan fraud) on a SAR, also indicate within the SAR that such a known or suspected violation is the result of identity theft or pretext calling. Specifically, when identity theft or pretext calling is believed to be the underlying cause of the known or suspected criminal activity, banks should, consistent with the existing SAR instructions, complete a SAR in the following manner:

- In Part III, Box 35, of the SAR check all appropriate boxes that indicate the type of known or suspected violation being reported and, **in addition,** in the "Other" category, write in "identity theft" or "pretext calling," as appropriate.

- In Part V of the SAR, in the space provided for the narrative explanation of what is being reported, include the grounds for suspecting identity theft or pretext calling in addition to the other violation being reported.

- In the event the only known or suspected criminal violation detected is the identity theft or pretext calling, then write in "identity theft" or "pretext calling," as appropriate, in the "Other" category in Part III, Box 35, and provide a description of the activity in Part V of the SAR.

Consistent with the SAR instructions, in situations involving violations requiring immediate attention, such as when a reportable violation is ongoing, a bank should immediately notify, by telephone, the OCC and appropriate law enforcement, in addition to filing a timely suspicious activity report.

VI. CUSTOMER ASSISTANCE

Teaching prevention

Educating consumers about preventing identity theft and identifying potential pretext calls may help reduce their vulnerability to these fraudulent practices. Banks should consider making available to their customers brochures, newsletters, or notices posted in their lobbies or on their Web sites describing preventative measures consumers can take to avoid becoming victims of

these types of fraud. Banks are strongly encouraged to inform their customers of the following precautionary measures that law enforcement recommends to protect against identity theft and pretext calling:

Do not give personal information, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet unless you initiated the contact or know with whom you are dealing.

Store personal information in a safe place and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away.

Protect your PINs and other passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc.

Carry only the minimum amount of identifying information and the number of credit cards that you need.

Pay attention to billing cycles and statements. Inquire of the bank if you do not receive a monthly bill; it may mean the bill has been diverted by an identity thief.

Check account statements carefully to ensure all charges, checks, or withdrawals were authorized.

Guard your mail from theft. If you have the type of mailbox with a flag to signal the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.

Order copies of your credit report from each of the three major credit bureaus once a year to ensure they are accurate. The law permits the credit bureaus to charge $8.50 for a copy of the report (unless you live in a state that requires the credit bureaus to provide you with one free copy of your report annually).

If you prefer not to receive preapproved offers of credit, you can opt out of such offers by calling 1-888-5-OPT OUT.

If you want to remove your name from many national direct mail lists, send your name and address to:
DMA Mail Preference Service
P.O. Box 9008
Farmingdale, NY 11735-9008

If you want to reduce the number of telephone solicitations from many national marketers, send your name, address and telephone number to:
DMA Telephone Preference Service

P.O. Box 9014
Farmingdale, NY 11735-9014.

Assistance for Victims

There are a number of measures banks can take to assist victims of such fraud. These include:

(1) having trained personnel respond to customer calls regarding identity theft or pretext calling;

(2) determining if it is necessary to close an account immediately after a customer reports unauthorized use of that account, and issuing the customer a new credit card, ATM card, debit card or checks, as appropriate. Where a customer has multiple accounts with an institution, the institution should assess whether any other account has been the subject of potential fraud; and

(3) educating customers about appropriate steps to take if they have been victimized.
The following are measures banks may advise their customers to take if they are the victims of identity theft.

Contact the fraud departments of each of the three major credit bureaus to report the identity theft and request that the credit bureaus place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud and the victim's statement asks them not to open additional accounts without first contacting you. The following are the telephone numbers for the fraud departments of the three national credit bureaus: Trans Union: 1-800-680-7289; Equifax: 1-800-525-6285; Experian: 1-888-397-3742.

You may request a free copy of your credit report. Credit bureaus must provide a free copy of your report if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing.

Review your report to make sure no additional fraudulent accounts have been opened in your name, or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries" and request that any inquiries from companies that opened the fraudulent accounts be removed.

Contact any financial institution or other creditor where you have an account that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account if there is evidence your account has been the target of criminal activity.

File a report with your local police department.

Contact the FTC's Identity Theft Hotline toll-free at 1-877-ID-THEFT (438-4338). The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.

The above measures are contained in a consumer brochure available on the OCC's Web site at www.occ.treas.gov/idtheft.pdf. Banks may download this information in the form of a trifold brochure and provide it to their customers.

Questions relating to this advisory should be directed to Amy Friend, assistant chief counsel, at (202) 874-5200.

_____
Nanette G. Goulet
Acting Deputy Comptroller
Community and Consumer Policy

APPENDIX: LIST OF OCC ISSUANCES REGARDING INFORMATION SECURITY

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information, 66 *Fed. Reg.* 8616, 8632 (February 1, 2001), to be codified at 12 CFR Part 30, App. B
- OCC Alert 2000-09:Protecting Internet Addresses of National Banks (July 19, 2000)
- OCC Bulletin 2000-14: Infrastructure Threats–Intrusion Risks (May 15, 2000)
- OCC Alert 2000-01: Internet Security: Distributed Denial of Service Attacks (February 11, 2000)
- "Internet Banking" booklet in *Comptroller's Handbook* (October 1999)
- OCC Bulletin 99-9: Infrastructure Threats from Cyber-Terrorists (March 15, 2000)
- Check Fraud–A Guide to Avoiding Losses (February 2000)
- OCC Bulletin 98-38: Technology Risk Management: PC Banking (August 24, 1998)
- OCC Advisory Letter 98-11: Pretext Phone Calling (August 20, 1998)
- OCC Advisory Letter 91-4 :Use of Social Security Numbers for Automated Call Systems (July 24, 1991)
- OCC Banking Circular 229: Information Security (May 31,1988)
- Banking Circular 226 :End-User Computing (January 25, 1988)

If You Become a Victim of Identity Theft

If you believe that someone has stolen your identity, you should:

- **Contact the fraud department** of each of the three major credit bureaus to report the identity theft and request that the credit bureaus place a fraud alert and a victim's statement in your file. The fraud alert puts creditors on notice that you have been the victim of fraud, and the victim's statement asks them not to open additional accounts without first contacting you.

  The following are the telephone numbers for the fraud departments of the three national credit bureaus:
  Trans Union: 1-800-680-7289;
  Equifax: 1-800-525-6285;
  Experian: 1-888-397-3742.

  You may request a free copy of your credit report. Credit bureaus must provide a free copy of your report, if you have reason to believe the report is inaccurate because of fraud and you submit a request in writing.

- **Review your report** to make sure no additional fraudulent accounts have been opened in your name, or unauthorized changes made to your existing accounts. Also, check the section of your report that lists "inquiries" and request that any inquiries from companies that opened the fraudulent accounts be removed.

- **Contact any bank or other creditor where you have an account** that you think may be the subject of identity theft. Advise them of the identity theft. Request that they restrict access to your account, change your account password, or close your account, if there is evidence that your account has been the target of criminal activity. If your bank closes your account, ask them to issue you a new credit card, ATM card, debit card, or checks, as appropriate.

- **File a report with your local police department.**

- **Contact the FTC's Identity Theft Hotline toll-free at 1-877-ID-THEFT (438-4338).** The FTC puts the information into a secure consumer fraud database and shares it with local, state, and federal law enforcement agencies.

Comptroller of the Currency
Administrator of National Banks

How to Avoid Becoming a Victim of Identity Theft

What is Identity Theft?

Identity theft is the fraudulent use of a person's personal identifying information. Often, identity thieves will use another person's personal information, such as a social security number, mother's maiden name, date of birth, or account number to open fraudulent new credit card accounts, charge existing credit card accounts, write checks, open bank accounts, or obtain new loans. They may obtain this information by:

- Stealing wallets that contain personal identification information and credit cards.
- Stealing bank statements from the mail.
- Diverting mail from its intended recipients by submitting a change of address form.
- Rummaging through trash for personal data.
- Stealing personal identification information from workplace records.
- Intercepting or otherwise obtaining information transmitted electronically.

Pretext calling is a fraudulent means of obtaining a person's personal information. Pretext callers may contact bank employees, posing as customers, to access customers' personal account information. Information obtained from pretext calling may be sold to debt collection services, attorneys, and private investigators to use in court proceedings. Identity thieves may also engage in pretext calling to obtain personal information to create fraudulent accounts.

Here are a few basic steps you can take to avoid becoming a victim of identity theft and pretext calling:

- **Do not give personal information**, such as account numbers or social security numbers, over the telephone, through the mail, or over the Internet, unless you initiated the contact or know with whom you are dealing.
- **Store personal information in a safe place** and tear up old credit card receipts, ATM receipts, old account statements, and unused credit card offers before throwing them away.
- **Protect your PINs and other passwords.** Avoid using easily available information, such as your mother's maiden name, your birth date, the last four digits of your social security number, your phone number, etc.
- **Carry only the minimum amount of identifying information** and number of credit cards that you need.
- **Pay attention to billing cycles and statements.** Inquire of the bank, if you do not receive a monthly bill. It may mean that the bill has been diverted by an identity thief.
- **Check account statements carefully** to ensure all charges, checks, or withdrawals were authorized.
- **Guard your mail from theft.** If you have the type of mailbox with a flag to signal that the box contains mail, do not leave bill payment envelopes in your mailbox with the flag up. Instead, deposit them in a post office collection box or at the local post office. Promptly remove incoming mail.
- **Order copies of your credit report** from each of the three major credit bureaus once a year to ensure that they are accurate. The law permits the credit bureaus to charge $8.50 for a copy of the report (unless you live in a state that requires the credit bureaus to provide you with one free copy of your report annually).
- **If you prefer not to receive preapproved offers of credit,** you can opt out of such offers by calling (888) 5 OPT OUT.
- **If you want to remove your name from many national direct mail lists,** send your name and address to:
  DMA Mail Preference Service
  P.O. Box 9008
  Farmingdale, NY 11735-9008
- **If you want to reduce the number of telephone solicitations** from many national marketers, send your name, address, and telephone number to:
  DMA Telephone Preference Service
  P.O. Box 9014
  Farmingdale, NY 11735-9014