Spotting and Avoiding Pretext Calls

All financial institutions need to be aware of the use of pretext calls by information brokers and identity thieves to gain unauthorized and often illegal access to customer information. The financial services industry takes the threat of unauthorized access to customer information seriously and was a leader in supporting the passage of the provisions within the Gramm-Leach-Bliley Act that make it a crime to obtain or attempt to obtain a customer’s information through the use of pretext against a financial institution or against the customer of a financial institution.2

All employees of the financial services industry need to:

1) Understand the definition of pretext as it applies to financial institutions;
2) Understand why pretext callers use pretext to access customer information;
3) Understand the types of pretext methods used;
4) Know how to spot possible pretext calls;
5) Know what to do when a possible pretext call is detected; and
6) Be aware of possible ways to stop pretext calls.3

Defining Pretext in the Financial Services Industry

Pretext is the use of deception to cover the true reason for a given action. Under Title V of the GLB Act, the use of pretext to illegally gain access to customer information maintained by financial institutions is a felony punishable by fine and/or imprisonment. Further, it is a felony to illegally induce the customer of a financial institution to reveal his or her own customer information. All employees of the financial services industry need to understand and be able to define pretext and pretext calls in order to protect customer information.

The most common pretext is a caller falsely informing an employee of a financial institution that the caller is a customer attempting to gain authorized access to his or her own information. The goal is to convince the financial institution employee to provide customer information that the employee would not provide if the employee knew the true identity of the caller. In many cases the pretext caller posing as a legitimate customer will have obtained some biographical and relevant account information from other sources or by means of identity theft in order to perform the pretext and further convince the financial institution that the pretext caller is the legitimate customer.

PRETEXT EXAMPLE

Bob Smith is the holder of an account at Main Street Bank. Joe Imposter obtains from various sources Mr. Smith’s full name, social security number, address, and date of birth. Joe Imposter, using pretext, calls Main Street Bank and identifies himself as Mr. Smith. The bank, for security reasons, asks for personal information that the bank mistakenly believes only Mr. Smith could know. Joe Imposter, armed with Mr. Smith’s biographical data, is able to convince the bank that he is actually Mr. Smith. The bank then provides Joe Imposter with any information he requests on Mr. Smith’s account.

---

1 This Training Manual was prepared by Robert Douglas, CEO, American Privacy Consultants, www.PrivacyToday.com, PO Box 2417, Alexandria VA 22301-0417, 703-836-8001.

2 SEC. 521. PRIVACY PROTECTION FOR CUSTOMER INFORMATION OF FINANCIAL INSTITUTIONS PROHIBITION ON OBTAINING CUSTOMER INFORMATION BY FALSE PRETENSES - It shall be a violation of this subtitle for any person to obtain or attempt to obtain, or cause to be disclosed or attempt to cause to be disclosed to any person, customer information of a financial institution relating to another person—(1) by making a false, fictitious, or fraudulent statement or representation to an officer, employee, or agent of a financial institution; (2) by making a false, fictitious, or fraudulent statement or representation to a customer of a financial institution; or (3) by providing any document to an officer, employee, or agent of a financial institution, knowing that the document is forged, counterfeit, lost, or stolen, was fraudulently obtained, or contains a false, fictitious, or fraudulent statement or representation.

3 See FDIC Financial Institution Letter (FIL) 98-98 for more information on pretext phone calls.
Pretext Calls are Used to Obtain and Sell Customer Information and for Identity Theft

Historically, information brokers, private investigators, collection agencies, and identity thieves have most commonly used pretext to obtain customer information from financial institutions.

The largest number of calls appear to be placed by information brokers who have developed a specialty in obtaining information on individuals and businesses and reselling it for a profit. Much of the information accessed and sold by information brokers is legally obtained from publicly available data that have been compiled into proprietary databases. However, prior to the passage of the GLB Act, it was determined that many information brokers were routinely advertising their ability to specifically obtain financial institution customers’ information. This information was being sold to anyone willing to pay for it.

Private investigators and collection agencies have also been traditional users of pretext to gain access to customer information. In many cases, attorneys or others seeking to locate the financial assets of an individual or business as part of a financial investigation have retained private investigators or collection agencies. Records obtained as part of investigations of the use of pretext have shown that pretext by private investigators and collection professionals is often used to determine if the customer of a financial institution has assets available to cover a monetary judgment entered by a Court, whether the customer has assets being hidden from a spouse or child, or is engaging in bankruptcy fraud by hiding undeclared assets.

Finally, identity thieves use pretext to obtain customer information as a means of committing financial crimes such as check and credit card fraud. Recent cases have disclosed identity thieves using pretext calls to financial institutions in order to raise credit card limits prior to using the credit cards to make illegal purchases or to illegally obtain cash.

Why Every Employee Should Care

The number of pretext calls to financial institutions can be conservatively estimated to be in the thousands of calls per day. In fact, the investigation and prosecution of just one information broker company determined that company was making hundreds of calls daily. Remember, there are tens of thousands of information brokers, private investigators and collection agencies in the United States today. This means that it is very likely that your financial institution has already been the target of pretext calls.

The types of financial information advertised for sale include: individual and business bank account numbers and balances; individual and business bank account transaction records, including monthly statements; stock, bond and mutual fund holdings, including the number of shares held; insurance policy data, including the types of insurance maintained and the amount or value of the policy; credit card information, including account numbers, size of credit lines; and transaction details, including specific purchases.

Today there are literally dozens of information brokers and private investigators advertising their ability to locate financial institution customer account information in the United States by means of the World Wide Web. Using just one of numerous Internet search engines, anyone can locate a website advertising the sale of financial institution customer account information. The advertisements almost uniformly refer to “bank account searches” and/or “asset investigations.” Not all of these firms are using pretext or violating the law, but investigations by state and federal authorities and the media have determined that many firms are in fact using pretext to gain customer information.

The financial services industry can address the threat by enacting security procedures designed to thwart pretext. The key is to balance customer information convenience with customer information security. By educating both financial institution employees and customers about the need for information security, the financial services industry will continue its leadership role in safeguarding customers’ assets and information.

The four steps used by a pretext caller are:

1) Decide what information is sought;
2) Identify the custodian of the information;
3) Identify who the custodian will release the information to and under what circumstances; and
4) Use a pretext to be that person under those circumstances.

There are a variety of pretext methods in use today, and the list continues to grow. Numerous books and training courses are available to those seeking to use pretext to gain unauthorized access to confidential information. Additionally, on a daily basis, new pretext methods and variations are traded in Internet discussion areas specializing in pretext and investigation.

While pretext methods vary, all pretext calls to the financial services industry have one common feature:

The individual illegally attempting to access customer information by placing a pretext call will try to convince the financial institution that the pretext caller is authorized to access the customer information.

In order to determine what pretext methods have the potential to defeat the institution’s customer information security procedures, the institution must first determine what individuals and/or entities are currently granted access to customer information and under what circumstances. Once a list is created of who has access to customer information and under what circumstances that access is granted, an institution can make educated decisions concerning what methods of pretext might succeed in defeating the current customer information security procedures. Further, the institution can take steps to further review and strengthen procedures for access to customer information. Remember that a pretext caller failing to get the desired information from one employee will often call employee after employee, using the same or different methods.

Traditionally, pretext callers have succeeded in using the following five general pretext methods to circumvent the customer information security procedures of a financial institution:

1) Impersonating a Customer. The most common pretext is the impersonation of a customer of an institution. The pretext caller will falsely state that he/she is the customer of the institution and needs to gain access to his/her account information. The pretext caller will often have the correct biographical information (name, address, phone number, date of birth, social security number) of the true account holder, having obtained this biographical information from public resources, proprietary investigative databases and identity theft.

However, in most pretexts the caller will be missing one or more pieces of information that are normally available to identify the caller as the account holder or that the institution requires in order to gain authorized access to account information. The most common missing pieces of information are account number; personal identification number (PIN); password; mother’s maiden name; amount or date of last deposit or withdrawal; the branch or address of the institution where the account was opened; or the date when the account was opened.

The pretext caller will attempt to convince the financial institution that there is a reason the caller does not have the needed information; that the pretext caller is in fact the customer; and that the institution should bend the rules and allow access to account information because there is a compelling reason to do so. Typical examples of reasons given may include:

- “I don’t have my account number because I don’t have my check book with me here at work.”
- “I can never remember that stupid PIN—I haven’t had to use it for the longest time.”
- “My mother’s maiden name is Smith.” (When informed that the name on record is different)
Who are you to tell me what my mother’s maiden name is? You must have written it down wrong on your end.”

- “Password? I can’t remember my password and I need this information right away or I’m going to start bouncing checks! Either give me my account information or I’m closing the account.”

- “I don’t have my account ledger here with me so how can I tell you my last deposit or withdrawal? Besides, my wife makes deposits and cashes checks all the time.”

- “Please—it has been so long since I opened the account I can’t remember where or when it was.”

Examples of Other Pretexts that are Considerably More Elaborate Include:

- “I’m on a business trip and don’t have my checkbook with me. I need to check my account balance in order to determine that a deposit was made so I don’t bounce any checks. My mortgage check is in jeopardy of bouncing so you must help me.”

- “I need to wire a large deposit to your customer, and the wire must happen today. Your customer is at the funeral of his mother, and I can’t reach him. He gave me his account number but it got wet, and I can’t read it. He needs this money to cover funeral expenses. You have to help me. I’ll be sure he knows what great assistance you provided in his hour of need.”

- “I’m at the office and don’t have my checkbook with me. I need to finish this car loan application and fax it in today. Can you please help me? I need my account number and balance right away, or I won’t be able to get this loan and close the deal.”

- “My wife and I separated several months ago, and she hasn’t been forwarding my mail. I need to balance my account so I don’t write any bad checks. I need you to fax the most recent copy of my statement to me here at the office.”

Often, the goal of the pretext is to obtain information one piece at a time. Once the pretext caller finds an employee who will assist with one piece of information (which may not even be account specific) the pretext caller will continue to ask questions to try to obtain all the information necessary to access the account.

2) Impersonating Another Official within the Institution. If a pretext caller has difficulty bypassing the customer information security procedures of an institution by impersonating the customer, the caller may attempt to impersonate another employee or official of the institution. Remember that step three of a successful pretext is identifying whom the financial institution will release the information to and under what circumstances. An employee will almost always respond to the request of an individual the employee believes to be their superior within the institution. Institutions with more than one branch or physical location have employees who do not know everyone within the employ of the institution. This makes an internal pretext possible.

Examples of this Form of Pretext in the Financial Services Industry Include:

- “Hi. This is Ann in Legal. I’m filling in today for Tracy and need to obtain some account information on John Jones. I have his social security number but can’t figure out how to locate his information here on the computer. Everyone else is at lunch, and I need this right away. Can you help?”

- “This is Bob with Customer Service over at the Park Avenue Branch. Our system just went down, and I have a distressed customer sitting in front of me that I need to help. Can you punch him up on your end and read me the following…”

3) Impersonating Another Institution. Another pretext that has been used with success for many years has been the impersonation of an employee of a separate institution. Many information brokers and identity thieves have learned that by posing as an official from another financial institution with questions
concerning a customer they can successfully perform a pretext on the customer’s institution. This method takes advantage of the natural inclination to assist another institution in day-to-day activities. Often in this method a false story will be developed to elicit the help of the institution in stopping a fraudulent transaction. The goal is to appeal to the good nature of the employee to assist in stopping the fraud.

Examples of this Form of Pretext in the Financial Services Industry Include:

- “Hi. This is Joe Jones over at Main Street Bank. Bob Smith, a customer of yours over there at 1st National Bank was in earlier and presented us with a check of yours that we had doubts about. Instead of completing the transaction, Mr. Smith walked out and said he would be back later. Can you bring up his account information and assist me in case he returns? We made a photocopy of the check before he left but the quality of the copy is poor, and we cut off the bottom so I don’t have his account number. I have his full name and address if that helps…”

- “Hi. This is Mary at Check Systems Fraud Department. We have some questions pertaining to a customer of yours…”

- “Hi. This is Bob with Sears Credit Card Collection and Skip Trace Department. It appears we have a mutual customer in John Jones. I need some information from you regarding his account and in return I may be able to alert you to some irregular financial activity on his part…”

4) Impersonating a Government Regulatory Agency.
While far less common, there are cases of pretext callers impersonating officials of government regulatory agencies. This form of pretext relies upon the recipient of the pretext call believing that the caller is an official needing access to customer information as part of an inquiry or investigation. Agencies reported to have been both impersonated and the recipients of pretext calls include the Federal Reserve, Federal Deposit Insurance Corporation and the Internal Revenue Service.

Remember that federal laws such as the Right to Financial Privacy Act prohibit the dissemination of information to government agencies by an institution unless there has been a search warrant, subpoena or administrative summons. Most government agents will understand your reluctance to provide such information over the phone.

5) Impersonating Law Enforcement Authorities.
A final method that is used is the impersonation of law enforcement authorities. Similar to Pretext Method #4 above, this form of pretext again relies upon the reality that many financial institution employees will assist someone in law enforcement. This pretext has worked even when institutions have strict guidelines that notify employees they are not to release information absent a subpoena or other form of court order. A call from a purported police officer or Secret Service agent in need of immediate assistance can be very unnerving to an employee and can prey upon the employee’s desire to assist law enforcement in preventing or solving a crime. Private investigators and private detectives have known for years that even when they properly identify themselves, whether by phone or in person, they are often mistaken for law enforcement officers. Unfortunately, there are unscrupulous private investigators and private detectives that have learned that by dropping the term “private,” or by overtly misrepresenting themselves as law enforcement personnel, they increase the likelihood of obtaining the information they seek.

Examples of this Form of Pretext in the Financial Services Industry Include:

- “This is Investigator Jones. I need assistance with a matter I’m working on that involves one of your customers. I need you to assist me with a quick piece of information.”

- “This is Detective Smith. We have your customer Mr. Jones in custody, and I need to verify his account number and balance. Mr. Jones is in the lock-up and claims he doesn’t remember his account number. I have his social security number and address if that will help you find the account.”
Spotting Pretext Calls

There are a number of indicators that what at first appears to be a routine and valid request for customer information may instead be a pretext call. The presence of any one of these indicators or a combination thereof does not always indicate a pretext attempt. Financial institutions receive numerous requests every day for customer information. In many of those requests one or more of the following indicators may be present and be perfectly innocent. However, financial institution employees should be aware of these potential indicators and review them on a regular basis in order to be prepared to spot a potential pretext.

Most important, remember that the pretext caller is a confidence artist. The basis of the confidence game for the pretext caller is to take advantage of the financial services industry’s reputation as customer service-oriented. By appealing to the emphasis placed on customer service within the industry, the pretext caller attempts to obtain information that he or she is not legally entitled to.

If it feels like a con – it probably is.

- **Missing Information**  Any call or request for customer information where the institution’s defined requirements for gaining access (PIN, password, last date of deposit and amount, etc.) are not met.

- **Non-customer Calls**  Any call where the person requesting the information is not the customer.

- **Calls Placed from Numbers Others Than Those Listed on the Customer’s Account**  If an institution has caller identification capabilities, employees should note whether the phone number displayed matches the phone number(s) associated with the customer account. Particular attention should be given to calls placed from outside the local calling area of the customer and calls that have been placed that block the caller identification feature.

- **Callers Who are Hesitant or Refuse to Give a Call-back Number**  Any caller that refuses or hesitates in providing the number they are calling from may be concerned about the call being traced back to them. Many pretext callers will immediately hang up if confronted with a courteous request for the number they are calling from.

- **Out of the Ordinary Request**  Any call that is out of the ordinary. This includes requests for faxes of account information or statements to numbers outside the local calling area of the customer and requests to mail duplicates of account information to an address other than that on the customer account.

- **Overly Aggressive Callers**  Any caller who becomes belligerent or aggressive when asked routine account identifying information. A favorite ploy of pretext is to bully the employee into releasing information by threats to speak to a supervisor, close an account or make a complaint about the employee.

- **Overly Talkative Callers**  Callers who appear to be laying out a story concerning why they need to bypass the access rules of the institution or who appear to be attempting to distract the employee with excessive chit-chat while posing more account-related questions may be constructing a pretext. The best pretexts lure the employee into providing information not even requested in an attempt to assist the confused caller.

- **Absentminded Callers**  Callers who appear to be overly confused or absent-minded and are unable to provide even basic biographical information may be placing a pretext call. Many pretexts rely on placing many calls to the institution and picking up one piece of information at a time until enough data are collected to convince the institution that the caller is the legitimate account holder.
Handling a Possible Pretext Call

All financial institutions should develop policies and guidelines for employees to follow when a pretext call is suspected. It must be stressed that the policies and guidelines are to be followed without exception by all employees of the institution. Considerations for policies and guidelines should include:

- **No Variation From Customer Information Access Procedures** Whatever customer information access procedures are determined to be appropriate for the individual institution should be strictly enforced. No frontline employee should have the authority to deviate from the stated procedures. Legitimate customers will appreciate security procedures when it is explained that the procedures are in force to protect their valuable information. Frontline employees should be instructed that they could be dismissed from their job for deviating from the institution’s customer information security procedures.

- **Routing Suspected Pretext Calls to a Supervisor Or Security Official** Any suspected pretext call should be brought to the immediate attention of a supervisor or security official within the institution and if feasible the call should be routed to that official. Many pretext attempts will end with a hang-up by the pretext caller as soon as a transfer to another official begins. Many pretext callers would prefer to end the call and try again at a later point than deal with a supervisory or security official.

- **Recording Suspected Pretext Calls** Where applicable state and federal laws permit, consideration should be given to recording any suspected pretext calls. Several successful prosecutions of pretext callers have been based upon recorded attempts at gaining access to customer information.

- **Notation Of Suspected Pretext Calls** At all times employees should make note of any suspected pretext call. If possible, notation should be on the individual account so that, if further attempts to gain access occur, other institution employees will be aware of the history of pretext attempts on the account. The notes should include the method of the suspected pretext. *Pretext callers will repeatedly call an institution and speak with different employees until they gain access. Notes on the account of attempted access can serve to notify other employees to give the account special attention.*

- **Request A Call-back Number** Requesting a call-back number will often assist in determining if the call is a pretext. Many pretext callers will immediately hang up when asked to provide a call-back phone number. If the number does not match the phone numbers associated with the account, ask the caller where they are and who is the owner of the call-back phone number. Most legitimate callers will not mind providing that information and will be impressed with your security efforts on their behalf.
Stopping Pretext Calls

As part of an overall security plan, consider the following elements covering pretext call prevention:

- **Customer Information Security Plan** The plan should address the threat of pretext calls to the integrity of a customer’s personal information and the reputation of the institution. You should determine who currently has authority to release information and under what circumstances the release can be made. Check that your procedures are consistent with current practice.

- **Do Not Deviate from Customer Information Security Procedures** Once a comprehensive plan has been developed it must be adhered to uniformly. Supervisors should demonstrate to frontline personnel that they take the procedures seriously by both following the procedures and enforcing them.

- **Use Authorization Codes or Passwords** Codes, passwords or other identifying information should always be used before any release of information by phone, fax or other telecommunication device.

- **Refer Questionable Calls to a Supervisor or Security Official** A supervisor or security official should handle all calls that are questionable or suspicious. The act of routing a call to a supervisor or security official will deter most pretext callers for fear of further scrutiny of their actions. Legitimate customers will appreciate the attention being provided to maintaining the integrity of their account.

- **Educate Employees** All employees are potential targets of pretext calls and should receive regular and repeated training to identify and handle pretext calls in conformity with your information security procedures.

- **Test Your Customer Information Security Procedures** Internal or third-party pretext testing should routinely evaluate your information security procedures. This will help identify weaknesses in procedures or training.

- **Educate Customers** Educate customers about the high degree of emphasis you place on protecting this information. Remind customers that they should never provide their customer information to anyone over the phone unless they initiated the call and are certain with whom they are dealing. When dealing with a difficult customer who wants access to information but is unable to provide appropriate identification, stress that the procedures of the institution are designed to protect their assets from identity thieves.

- **Report Suspicious Advertisements by Information Brokers, Private Investigators, Collection Agencies and Others** Look for advertisements in local publications, trade journals, magazines, yellow pages and on the Internet referring to the ability to locate “assets.” Pay particular attention to advertisements claiming to be able to locate account, credit card, stocks, bonds, mutual funds and insurance information. Users of pretext are notorious for claiming that they follow all laws and require appropriate documentation. Report suspicious advertisements to local and federal law enforcement and regulatory bodies including the Federal Trade Commission.

- **Report Pretext Attempts to the Appropriate Authorities** If you determine that a pretext caller is targeting your institution, you should contact your regulator or, if you believe that the pretexting is being done to commit a fraud, consider filing a Suspicious Activity Report (SAR) with the Treasury’s Financial Crimes Enforcement Network. While the filing of a SAR is not required, the agencies may issue a guidance encouraging the filing if a potential identity theft is involved. You may also wish to contact the FTC, which is keeping information on identity theft cases, at 1-877-IDTHEFT. Prosecution can also be an effective deterrent. For example, most information brokers and private investigators are refusing to accept asset investigations in the State of Massachusetts because of the State’s aggressive prosecution of pretext callers.