



Pretexting

*William Lafferty, Colorado
and
Carl Determeyer, Washington
April 2008*

Information Protections



The Weak Link In Our Security? Human Nature!





Pretexting

Definition: Pretexting is “the act of creating and using an invented scenario (the *pretext*) to obtain information” from a *target*, usually over the telephone.

Pretexting is more than a simple lie. It involves prior research, identifying needed data, crafting a believable story, & play acting.

The pretexter uses pieces of information to:

- Establish legitimacy in the mind of the target
- Manipulate people into revealing confidential information

Who *is* this “target”? Your Agency. Your Staff. Even YOU!

SWA's Pretexting Case

All 50 states were hit!

State	Number	State	Number	State	Number	State	Number
Alabama	277	Iowa	722	Nevada	289	Tennessee	331
Alaska	17	Kansas	160	New Jersey	197	Texas	2809
Arizona	204	Kentucky	254	New Mexico	331	Utah	170
Arkansas	713	Louisiana	163	New York	126	Vermont	65
California	1181	Maine	139	North Carolina	118	Virginia	787
Colorado	475	Maryland	477	North Dakota	46	Washington	1607
Connecticut	328	Massachusetts	50	Ohio	552	West Virginia	229
Delaware	113	Michigan	1869	Oklahoma	207	Wisconsin	523
Florida	156	Minnesota	380	Oregon	321	Wyoming	69
Georgia	659	Mississippi	732	Pennsylvania	533		
Hawaii	9	Missouri	216	Person	39	Others	Number
Idaho	221	Montana	104	Rhode Island	14	Banks	9836
Illinois	1769	Nebraska	294	South Carolina	108	Defense Dept & IRS	160
Indiana	1108	New Hampshire	65	South Dakota	71	SSA	960



Pretexting

A pretexter needs to appear “normal”, to not “stand out”, to “blend in with the crowd”. The commonplace is rarely noticed; the routine and mundane are quickly forgotten.

Pretexting is a form of *Social Engineering*

- ❑ These are *psychological attacks* - *manipulation*
- ❑ They use persuasion, ingratiation, helplessness, and friendliness



Colorado Call Recording Process

- Captures call from delivery to agent to disconnect
- Records customer side of conversation during hold time
- Captures data about the call: caller ID, date/time, duration, agent
- Records the data in the QCM system and a contact log in the front end GUI
- Calls can be retrieved by agent, date(s), time or caller ID
- Calls can be saved as .wav files for later playback
- Calls can be used for agent QA reviews, threat situations, scams, fraud
- Record 100%!



WHY Call UI?

There are many reasons a pretexter calls
(all nefarious):

Identity Theft

Skip Tracing

Fraudulent UI Claims

Data Mining

Recordings – How good are they?

The answer is *very good*. Lets listen to some actual calls.



Should I Be Concerned? YES!

If this group learned how to take advantage of **UI, ES, IRS, SSA, Hospitals, Banks**, etc., *others can too!*

Social engineering is a huge threat – it's the new “wave” in fraud. Pretexters can compromise your security & breach confidentiality in minutes; without you even knowing security was breached, and without you ever knowing someone “gave away the farm”.

Failing to address this threat could result in fraud, bad press, or even litigation.



What To Do To Guard against Pretexting

- ❑ Be on guard when a caller seems to be fishing for specific information without really providing you with anything confirming their identity.
- ❑ Have the caller verify enough information that their identity is established to your satisfaction. Trust your instincts – if you have doubts, *ask more questions*.
- ❑ Do not be shy about questioning a caller in-depth when the identity is in question. A real caller will appreciate the fact that you are protecting their confidential information. A pretexter will grow frustrated, evasive, and will eventually hang up.
Encourage the caller to file a claim (more on this later)



What To Do to Guard against Pretexting

- Maintain control of a call – do not let the caller “steer” you or take over the call. Do not be intimidated by aggressive tactics. Remain calm and professional, but firm.
- Be aware of your biases, how your experience and expectations shape your judgment.
- Maintain a list of the known or **suspected** phone numbers the pretexters are using for your staff to reference.
- Never volunteer more information than the caller has already verified. Most claimants know *that* they worked, *where* they worked, and *who* they worked for.



What To Do to Guard against Pretexting

- ❑ Pretexters want information – they do not want to file a claim. Offer to file a claim, ask for a name and address, ask them for specifics. Genuine claimants provide it, pretexters avoid it. If they use the, “But I need to know which state to file in” line, tell them you’ll take the claim and if it turns out it should be filed against another state, you’ll handle it.
- ❑ Be wary of callers that lead you down a path or line of inquiry too quickly. Pretexters will typically have you looking for wages within the first minute of the call - genuine claimants are still asking very basic questions at this point. Offer to “research” the issue with the other state and call them back. Pretexters do not give out genuine phone numbers, lest they be tracked and identified.



Pretexting

- ❑ The organized theft of records covered by privacy laws has become one of the fastest growing and least prosecuted crimes.
- ❑ Now, the continuing furor over HP's involvement in pretexting offers a wake-up call for everyone as to just how widespread the problem is, and how easy it is to pull off.
- ❑ Congressional Committee (CC) pretexting hearing:
 - ❑ Congressional documents show companies hire private investigators, who hire data brokers, who then hire even seedier contractors.
 - ❑ Majority of those questioned by the CC took the Fifth



Pretexting Laws and Cases

- ❑ Gramm-Leach-Bliley Act Federal and state crime to pretext for financial records
- ❑ Federal Crime to pretext for telephone records.
 - HP case
- ❑ State of Florida vs. Global Information Inc. Global was an Information Broker operating in Florida. Wachovia bank utilized services to the tune of \$456,250 obtaining information by their auto lending division. The fine was \$250,000



Pretexting Laws

Title 42 USC, section a, paragraph 6

“Willfully, knowingly, and with intent to deceive the Commissioner of Social Security as to his true identity (or the true identity of any other person) furnishes or causes to be furnished false information to the Commissioner of Social Security with respect to any information required by the Commissioner of Social Security in connection with the establishment and maintenance of the records provided for in section 405(c)(2) of this title;...”



Employment Security Department's Pretexting Case

Fall of 2005 first calls came in to WAESD. Calls were suspicious in nature, callers not interested in filing a claim, phishing for information. Colorado sends alert through IPC network (also getting calls since fall '05).

Several phone numbers identified. Decision was made to allow calls to continue. Colorado shares recordings.

An OSI Investigator speaks at the Chicago UI Integrity Conference. Numerous other states are now reporting calls from these numbers. Multi-state investigation.

Summer of 2006 "Bad Guy" Communication Records were subpoenaed.

Results of Subpoena

From 11/2005 through 10/2006, there were 49,523 outgoing phone calls from the bad guys, BNT Investigations.





Findings

Calls were made to all 50 State Workforce Agencies, the IRS, SSA, DOD, Banks, Hospitals, plus other public and private entities.

March of 2007 Federal Agents from DOL, IRS and SSA OIG join the investigation. This is a ground breaking case for all.



April/May 2007

Surveillance of known location in Belfair, WA continues. 20 Employees identified

A second location was discovered, business was booming

Federal Search Warrants obtained for both locations

May 8, both locations searched by SSA, DOL, Treasury, WSP and OSI Investigators

Hiding in middle America



A Second Location





Worked from a “Call Center”

Cubicles were equipped with telephones. Employees were given daily lists of calls to make.

The office manager for each location had the computers and controlled the work loads.

Employees were reminded to change their stories and avoid repeating the same theme too often.

They had lists of local call center offices, which were good ones to call and who to talk to in the office to get the best information.

They had gone so far as to make up their own shirts, with an embroidered badge and “BNT Investigations” on it.



May/Summer 2007

Large number of boxes containing information were seized, more employees identified.

People/Companies further up the chain identified. These people in WA were the bottom feeders.

Based on information gathered in Western Washington, search warrants executed in other states - New York, Texas, and CA.



December 2007

10 Initial Indictments Nationwide

BNT Investigations, Belfair, Washington

Brandy and Emilio Torrella-Owners

Steven Berwick-Office Manager

Private Investigators from Other States

California, Oregon, Texas, New York

Ten People Initially charged. However, the investigation continues.



Themes Used

Callers told the IRS they had fired their bookkeeper and needed their tax information to verify records.

Claimed they were a battered spouse and needed the information to avoid more beatings.

Called pharmacies posing as a representative of a doctor's office and stated they were authorized to obtain this information.

Callers used tears to appeal to emotional responses of the agents.



More Themes

Callers told the IRS they were in a hospital emergency room and needed surgery. They needed the tax information to verify income for the hospital.

Callers told UI that they just moved, wages were reported under wrong SSN, the employer's accountant had "messed up".

When the call center agents asked tough questions, the callers distracted them with embarrassing assertions. These included being a battered spouse, having a child abducted, experiencing bankruptcy, foreclosure or a serious illness.



Even More Themes

“I had an accident and have amnesia”.

They would play the flirty female or the “dumb blonde” role (“Elsa/Lisa/Brandi”).

The caller would act like a pot head.

Also used an Attention Deficit Disorder theme, the FBI witness protection program and mental retardation among others.

The key was to alternate themes and never repeat them to the same office.



Reverse Scripts

The “bad guys” were not above calling the object of the investigation.

Usually with a story like “Hi, my name is XXX from the State of YYY UI office. Your employer overpaid UI taxes and we have a check for you.”

They would then proceed to have the victim give their employer and employer's phone number, with a promise they would see the “check” in 4-6 weeks.

Why Information Theft?

Money, money, and more money

Current Employment Information \$30- \$75.

Banking Information \$100.00 per bank.

Tax Information \$250 to \$300

Medical Information \$50

5 years of comprehensive medical
information \$150

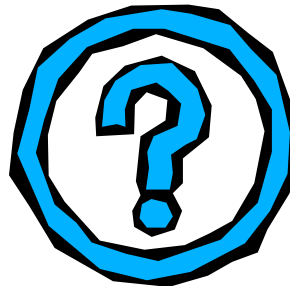
Asset Search \$300



Lessons Learned

- Do not turn off receiving calls – Document Calls
- Train your TeleCenter Agents and other staff what to listen for, look for, and how to handle the call
- Develop procedures for Call Center staff
- Assign a resource to track, analyze, and investigate
- Identify laws to use - criminal charges vs. civil suit
- Find a prosecutor – work with Federal staff

Pretexting



*William Lafferty, Colorado
and
Carl Determeyer, Washington
April 2008*