

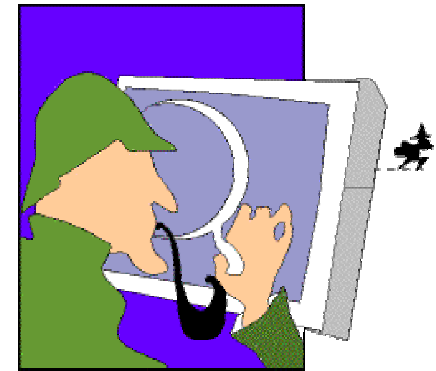
Identity Theft Wireless Threats and Defenses

Presented December 7, 2004

By

Peter Tapling
Authentify, Inc.

ACSAC 2004
Tucson, Arizona



ID Theft – What is it?

- IDENTITY THEFT is the use of personally identifying information belonging to one individual by another individual for financial or personal gain.

 - It is **not**
 - Bad charges on an existing credit card
 - Passing forged checks on an existing checking account
-

Lost Control of Your Own Identity

- For all practical purposes Identity = Social Security Number
 - This is a big part of the problem!
 - Easy for identity thieves to assert they are someone else with the right data
 - Difficult for Identity Theft victims to prove that they are themselves once compromised
 - New threat of “Identity Theft Fraud” from consumers attempting to evade legitimate debts
-

“Types” of ID Theft

Financial

- Thief uses your name and credit to their financial benefit.
- Establishment of new accounts based on victim's personally identifying information (cards, cars, houses, utility service, etc.)

Counterfeit Character

- Thief uses your name and identity information as their own for non-financial purposes
 - Use victims personally identifying information to rent home, provide to law enforcement, gain employment.
-

The Numbers

- ❑ 10 million individuals affected
- ❑ \$48,000,000,000 in economic losses
- ❑ 13 months before discovery
- ❑ \$5000 to \$90000 in fraudulent financial transactions
- ❑ \$600 to \$1500 out-of-pocket cost to fix
- ❑ 200 to 500 hours of time to fix
- ❑ 768,000 hits on Google search for "identity theft" OR "ID theft"
- ❑ 7,000 cases of mortgage fraud in '03; 24,000 in H1'04
- ❑ Maureen Mitchell case, see full testimony at:
http://commdocs.house.gov/committees/bank/hba92902.000/hba92902_0.HTM#44

More Sobering Numbers

- Two of the largest card issuing banks
- Losses ~\$600,000,000
- Between them ~300 million cards

THAT'S ONLY \$2 PER CARD!

Case Study – Maureen Mitchell

- Couple from Ohio
 - Alerted to situation by collections call
 - Could not get Law Enforcement to act
 - Pursued at their own expense
 - Perpetrator prosecuted
 - Perpetrator released after 2 years, immediately starts using same information to continue fraud

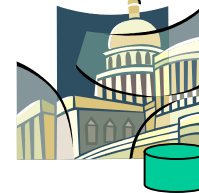
 - See full testimony at:
http://commdocs.house.gov/committees/bank/hba92902.000/hba92902_0.HTM#44
-

Actors in the ID Theft Play

YOU



Government



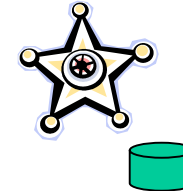
Financial
Institutions



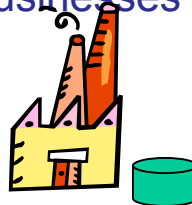
Personal
Business



Law Enforcement



Non-Financial
Businesses



THIEVES



What has changed? Why now?

- More reliance on data which is collected by more people and stored in more places
- Reliance on information over relationship
 - Mechanization, Electronic Commerce
- Lack of pursuit
- Individual → Organized

The Internet has not "caused" the ID Theft problem, but it has certainly increased its velocity.

Pay-off is High and Risks are Low

- Does not require temperament for violent crime
 - Does not require temperament for burglary
 - Unsuccessful attempts are essentially risk-free
 - Responsible identity thieves rarely apprehended
 - Low priority for law enforcement
 - Cross-jurisdictional challenges
 - Few incidents investigate
 - 1 in 700 incidents result in prosecution
 - Penalties are light
 - Identity thieves often released on bail

 - New attacks can succeed after initial detection of identity attack
-

Misguided Appraisals

- Identity theft happens when stupid consumers give their information to thieves.
- Identity theft is no larger a problem than other forms of fraud.

- "Preventing identity thieves from obtaining Social Security numbers will help to protect consumers from this pernicious crime."

FTC Commissioner Thomas B. Leary in Congressional Testimony 9/04

How is Data Compromised?

- "Known party" theft
- Insider theft
 - Temp administrator at your dentist
 - Rogue call center rep at your bank
- Dumpster diving
- Telephone service request
- Phishing, Spoofing
- Sniffing

These are of particular interest in the wireless world



Phishing / Spoofing

- Phishing is the use of a seemingly legitimate email/web requests to get an individual to provide confidential information
 - Spoofing is the establishment of an Internet based presence which appears to be that of an existing legitimate business in an effort to capture confidential information from customers of the legitimate business.

 - Focus is to get access to information
 - Some ID Theft, but not all
-

How bad is it?

- Fighting phishing/spoofing currently ranks as the #1 problem faced by risk managers in large financial institutions
 - One phishing attack can generate 30,000 calls to a customer service call center
 - A spoof site is generally up for less than 48 hours
 - The site spoofed may not be the site attacked
 - Investigation hampered by embarrassment

 - Gartner says that 30,000,000 people received phishing emails and 1,780,000 responded (12 months ended Apr 2003)
-

Characteristics of Phishing E-mail

E-mail spoofs trusted domain for sender e-mail address.



Utilizes visual cues to spoof authenticity of source.

Purpose: Service alert, system upgrade - need to reactivate account.

Ease of use - provides link to spoof site, masking real domain with trusted domain.

Provides working phone number for customer service back-up. In this case, the number goes to NetBank.

Date: Tue, 20 May 2003 16:40:07 -0400 (EDT)
 From: customersupport@bankofamerica.com
 To: Scobb <scobb@2cobbs.com>
 Reply-To: customersupport@bankofamerica.com
 Sender: customersupport@bankofamerica.com
 Subject: Security Server Update

Dear Valued Customer,

- Our new security system will help you to avoid frequently fraud transactions and to keep your deposited funds in safety.

- Due to technical update we recommend you to reactivate your account. Click on the link below to login and begin using your updated Bank of America account. To log into your account, please visit the Bank of America website at:
<https://www.bankofamerica.com/index.html>

To review your statement, log into your Bank of America account and click the eStatements & eNotices button in the left navigation of your Account Summary page. Your new statement is listed in the left navigation of the page.

If you have questions about your online statement, please send us a Bank Mail or call us at 1-888-BKONWEB (256-6932).

We appreciate your business. It's truly our pleasure to serve you.
 Bank of America Customer Care
 This email is for notification only. To contact us, please log into your account and send a Bank Mail.

A Sample Spoof Site



The image shows a spoofed version of the Citi website. The layout includes a top navigation bar with the Citi logo and links for 'sign on', 'open account', and 'contact us'. Below this is a main navigation menu with categories like 'PRODUCTS & SERVICES', 'PLANNING & TOOLS', 'INVESTING & MARKETS', and 'HELP DESK'. The central content area features a 'sign on to Citibank' form with fields for 'Card #/CIN' and 'PIN', and a 'sign on' button. To the left, there's a 'Welcome' message with a woman's image and a 'look for a product or service' dropdown. To the right, there's a 'sign on to your accounts' section with a 'Choose one' dropdown and 'learn more' and 'apply now' buttons. Below the main content, there are four promotional banners: '\$75 just for you.', 'Bank online en Español!', 'Citi® Platinum Select® Card' with '0% APR*', and 'There are many lessons to be learned. Apply for a CitiAssist® Student Loan Online - Get a response in 3 minutes.' Each banner includes a 'details' or 'apply now' link.

Why Does This Succeed?

- Spoof/counterfeit e-mail does everything an authentic e-mail does.
 - Source of e-mail verified by sender domain in "from" field
 - Source verified by visual cues - logo and graphics (consistent with Web graphics)
 - Service alert not inconsistent with offerings/planned offerings
 - Provides link to "safe" site.
 - Provides phone number for customer service
 - Tone is courteous and helpful
- Spoof site not inconsistent with legitimate site.
 - Visual/graphic cues for authenticity.
 - Information sought is not inconsistent with current and/or past bank practices.
- Social engineering, in the absence of secure, verifiable assertions of authenticity, is highly effective in deceiving the intended target.

Current State

- Organizations use email for multiple purposes
 - Environments
 - Authenticated - communication occurs within org's infrastructure after customer has authenticated
 - Unauthenticated - communication occurs via internet mail utilizing SMTP (Simple Mail Transport Protocol)
 - Contexts
 - Solicited, Unsolicited
 - Purposes
 - Sales, Fulfillment, Service
- Spoofing incidents experienced to this point have all been *unauthenticated, unsolicited, service* e-mails.
- SMTP (industry standard for internet e-mail) provides no process for verifying validity of identity assertions.
 - Lacking some process for verifying validity of identity assertions, any outbound e-mail we send via SMTP can be spoofed.
- The only process in place for verifying identity assertions is secure messaging process – Digital Signatures and PKI.

Sniffing

- “Listening” to network traffic
 - Means of harvesting email addresses generally
 - Unsecured wireless networks
- Keyboard loggers
 - Can be downloaded during mock “registration” event



Risk Factors Unique to Wireless Networks

- Assumption of “secure infrastructure” goes away
 - Open connection is by default bi-directional
 - WAP not perfect, but better than nothing
 - “g” and “i” specs getting better
 - VPN – most do not support “surfing”
 - Beware of replay attack
 - Login event could be point of compromise
-

Defense tactics

□ Passive, Active, Pro-Active

– Passive

- Try to deny identity thieves the information they need to attack

– Active

- Defeat an attack in progress by determining that information submitted is from an identity thief rather than the real consumer, or detect that previous attacks have succeeded soon enough to limit their damage

– Pro-active

- Prevent the attack from ever happening by making identity information unusable by anyone but its true owner, regardless of how complete the information, and regardless of their “human engineering” skills of the thieves
 - YOU need to be a part of this
-

Defense tactics

□ Passive, Active, Pro-Active

– Passive

- Try to deny identity thieves the information they need to attack

– Active

- Defeat an attack in progress by determining that information submitted is from an identity thief rather than the real consumer, or detect that previous attacks have succeeded soon enough to limit their damage

– Pro-active

- Prevent the attack from ever happening by making identity information unusable by anyone but its true owner, regardless of how complete the information, and regardless of their “human engineering” skills of the thieves
-

Passive Defenses

- Passive defenses
 - “Consumer Caution” (e.g., everyone buys a shredder)
 - “Institutional Caution”
 - Restrict access to paper records
 - Adequate security for electronic records
 - Passive defenses have failed and cannot be made to work
 - Identity information can be obtained from the consumers themselves via “human engineering” attacks
 - Identity information is too widely distributed/cannot be secured against dishonest insiders
 - Passive defenses do not expose identity thieves to detection
-

Active Defenses

- Active defenses
 - Data analytics (pattern recognition)
 - Vary authentication requirements by risk model
 - More rigorous authentication processes
 - Approaches range from requesting “harder to know” data to multi-factor authentication to biometrics
 - Active defenses are “Good Practice”
 - Some now mandated by FACTA
 - Detect breaches in the pro-active defenses
 - Best still let double-digit percentage of attempts through
 - None generate biometric audit trail for deterrence / prosecution
 - Rate of Identity Theft attempts rising faster than efficacy of active defenses -- “arms race” with identity thieves
 - More-aggressive active defenses generate more false negatives
-

Pro-Active Defenses

- Pro-active defenses
 - The ideal -- make the crime impossible/expensive to commit
 - The better the “pro-active” defense, the less passive and active defenses are needed
 - Private sector “large scale” proposals:
 - Professor Lynn Lopucki of UCLA School of Law
 - http://papers.ssrn.com/sol3/papers.cfm?abstract_id=263213
 - Robert Pinheiro, Independent Security Consultant
 - http://www.jecm.org/archives/04_vol2_issue1_art2.pdf
 - Jim Woodhill, Chairman of Authentify
 - **National Identity Theft Defense System**
 - Pro-active solution can not come from one company
 - Will require cooperative industry effort
 - Possibly mandated by legislation
 - No proposals for pro-active defenses were brought to the attention of Congress during the hearings leading up to FACTA, despite testimony from FTC, FRB, Dept of Treasury, etc.
-

The “Big Disconnect”

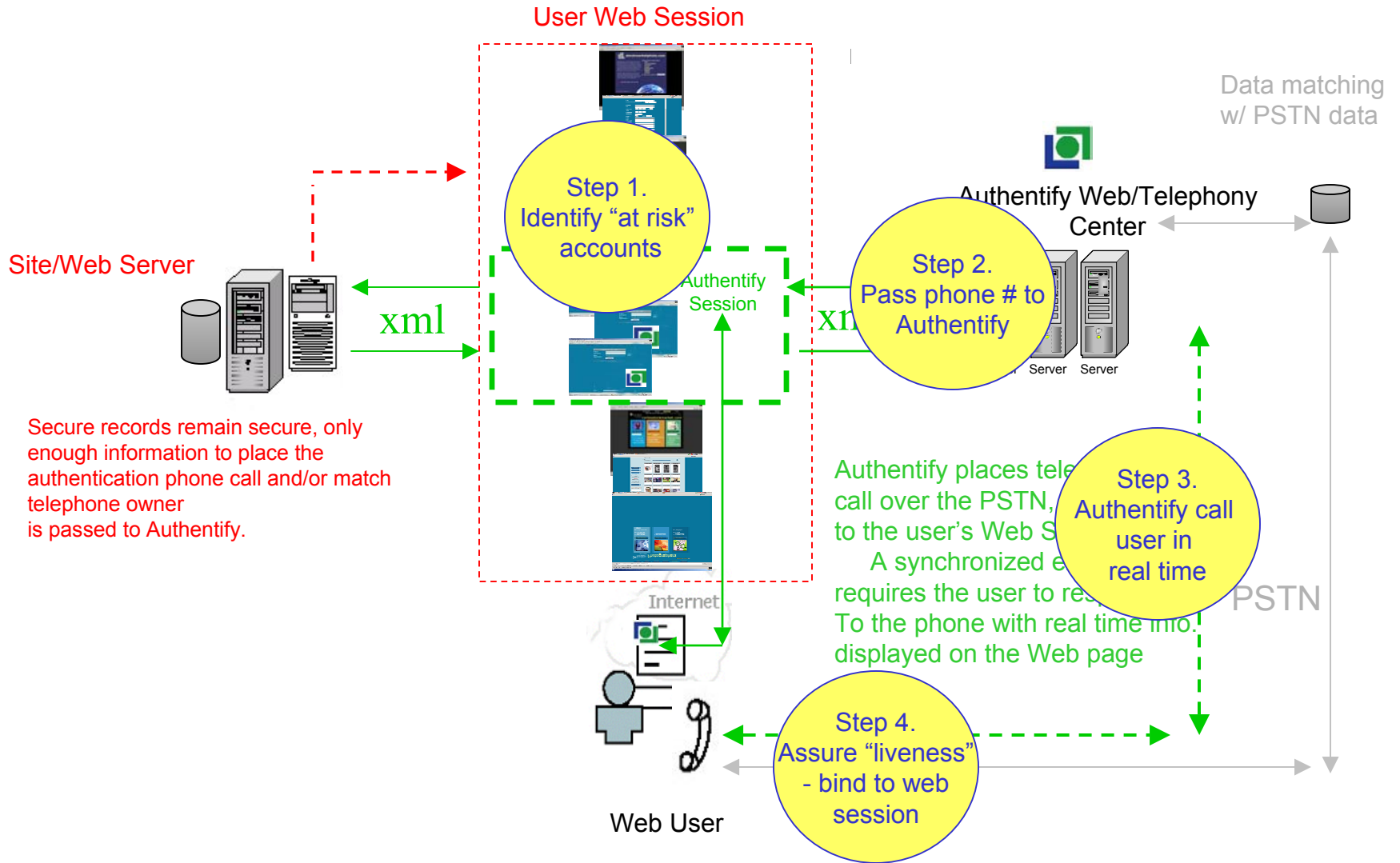
- Crime of Violence vs. Financial Crime
 - Huge numbers of victims will [and have already begun to] drive legislative change
 - Behavioral change will take longer
-

Financial Industry is Key

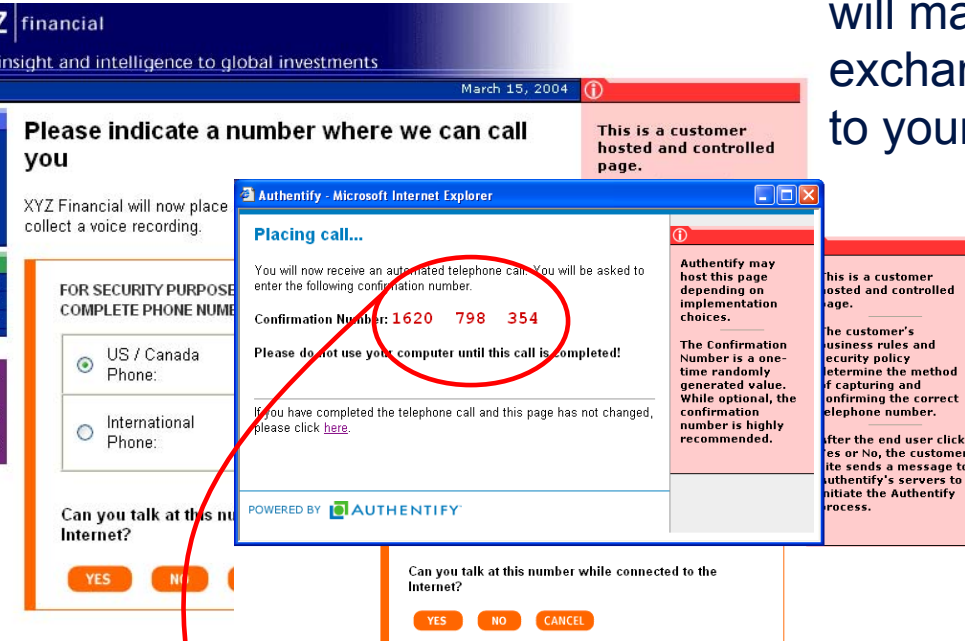
- Most ID Theft is financial in nature
 - When a bank opens an account or lends money in your name and it's not you, they have chosen to take the risk.
 - While central to the issue -- the problem is not their "fault"
 - Credit Reporting Agencies must be held accountable
 - Financial industry must play a lead role in any solution
-

“Solutions” in the Market

- Citibank ID Theft Protection program (best commercials!)
 - MasterCard SecurCode, Verified by Visa
 - Credit watch services
 - ID Theft insurance
 - Spyware detection software
-



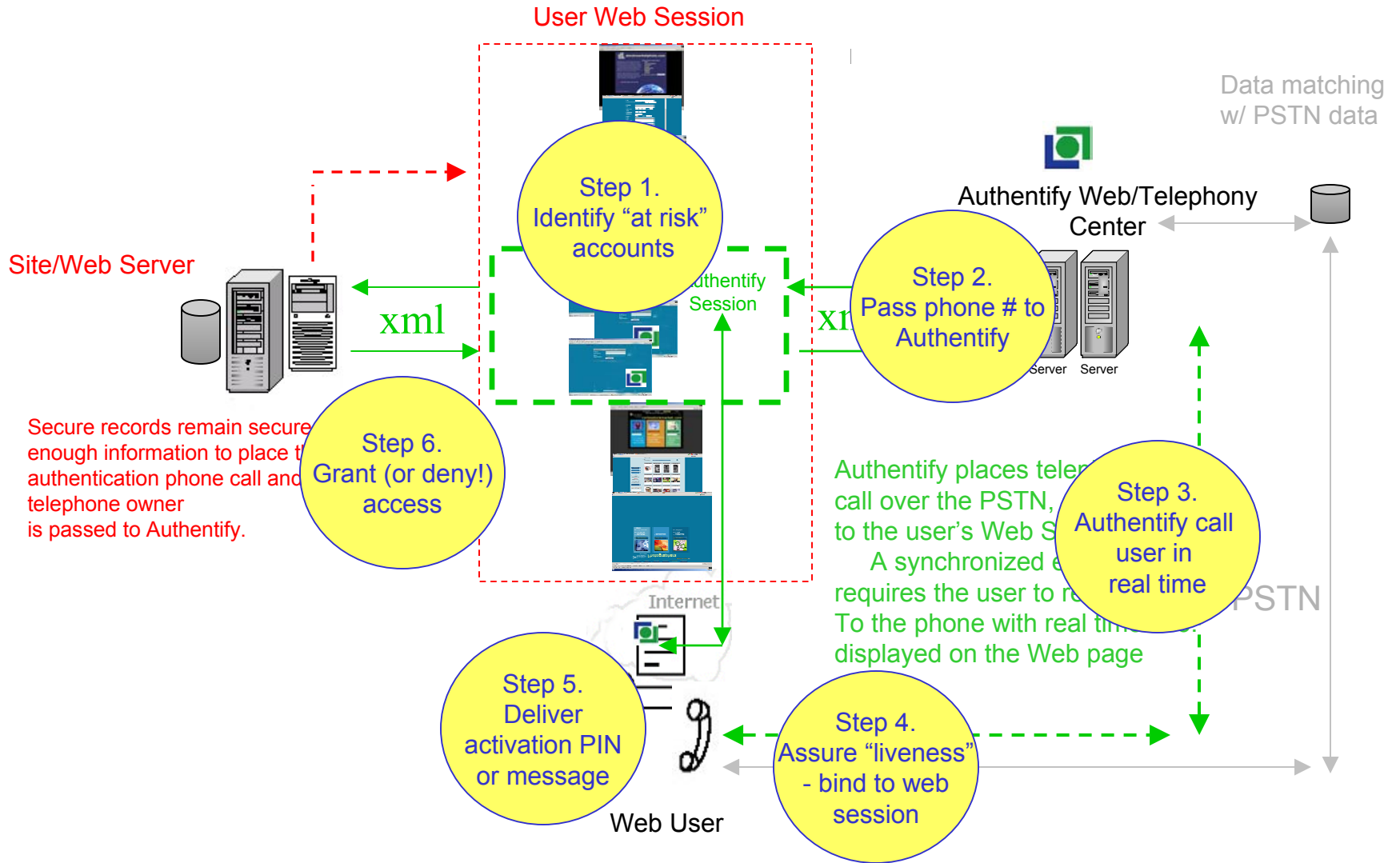
The Authentify authentication platform will manage the telephone call, and the exchange, providing an outcome status to your Network/Web server...



The screenshot shows a web browser window titled "Authentify - Microsoft Internet Explorer" displaying a security page. The page content includes:

- Header: "XYZ financial" with the tagline "Bringing insight and intelligence to global investments" and the date "March 15, 2004".
- Left sidebar: "Contents" (About XYZ Financial, Investment Accounts, Retirement Accounts, XYZ Financial Advisors, Contact US) and "Market Snapshot" (DJIA: 11,109.52 +83.62, NASDAQ: 3,929.5 +23.56, S&P500: 1,509.83 +5.62).
- Main content: "Please indicate a number where we can call you". Below this, it says "XYZ Financial will now place collect a voice recording." and "FOR SECURITY PURPOSES COMPLETE PHONE NUMBER".
- Form: Radio buttons for "US / Canada Phone:" and "International Phone:". Below the form is the question "Can you talk at this number while connected to the Internet?" with "YES", "NO", and "CANCEL" buttons.
- Confirmation dialog: A blue-bordered box titled "Placing call..." contains the text: "You will now receive an automated telephone call. You will be asked to enter the following confirmation number." followed by "Confirmation Number: 1620 798 354" (circled in red). Below this, it says "Please do not use your computer until this call is completed!" and "If you have completed the telephone call and this page has not changed, please click [here](#)." At the bottom of the dialog is the "POWERED BY AUTHENTIFY" logo.
- Warning boxes: Two pink boxes with information icons. One says "This is a customer hosted and controlled page." The other says "Authentify may host this page depending on implementation choices. The Confirmation Number is a one-time randomly generated value. While optional, the confirmation number is highly recommended." A third pink box on the right says "This is a customer hosted and controlled page. The customer's business rules and security policy determine the method of capturing and confirming the correct telephone number. After the end user clicks Yes or No, the customer site sends a message to Authentify's servers to initiate the Authentify process."

The user will speak a confirmation number into the telephone as it is displayed on their computer screen. The Authentify transaction manager will be waiting to recognize that number...



User Web Session

Data matching
w/ PSTN data

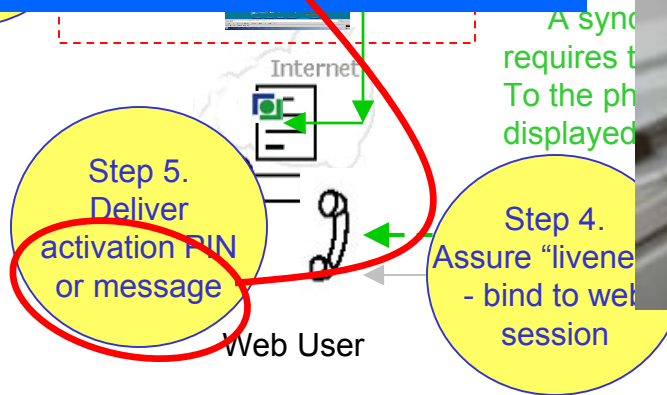
Message Delivery can include a recording the user left behind on a previous visit.

A deceptively powerful way to validate your site to them that doesn't rely on an exchange of personal information!

Authentify Web/Telephone

Step 5. Deliver activation PIN or message

Step 4. Assure "liveness" - bind to web session



Law Enforcement

- Law enforcement is needed to buttress any defensive efforts
 - Laws have been recently passed
 - Fair and Accurate Credit Transactions Act (FACTA)
 - http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=publ159.pdf&directory=/diskb/wais/data/108_cong_public_laws
 - ID Theft Penalty Enhancement Act
 - http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.21&filename=publ275.pdf&directory=/diskb/wais/data/108_cong_public_laws
 - Resources/jurisdiction still a major issue
 - US Postal Service Postal Inspector crosses boundaries
-

How Do I Protect Myself, My Family?

□ Things you **should** do...

- Protect basic information
- Review statements monthly; Limit number of relationships
- Review credit reports regularly
 - www.annualcreditreport.com
- Install/use SpyBot & Ad-Aware
 - www.safer-networking.org/en/home/index.html
 - www.lavasoftusa.com/support/download/

□ Things you **can** do...

- Insist on “out of band” confirmation of important transactions
 - Place “fraud alerts” with credit agencies
 - Credit watch services
 - ID Theft insurance
 - Write your legislative representatives
-

In Closing...

- DON'T PANIC!
 - ID Theft is not a “new” concept, but its velocity is alarming
 - There are simple things you can do to protect yourself
 - Federal Reserve Handout
 - <http://www.occ.gov/consumer/PhishBroch-Print1.pdf>
-

Resources

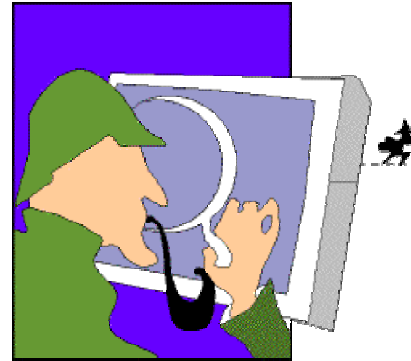
- FTC: <http://www.consumer.gov/idtheft/>
- FBI: <http://www.ifccfbi.gov/>
- US Postal Service: http://www.usps.com/postalinspectors/id_intro.htm
- SSA: <http://www.ssa.gov/pubs/idtheft.htm>
- Dept of Justice:
 - <http://www.usdoj.gov/criminal/fraud/idtheft.html>
 - <http://www.ojp.usdoj.gov/ovc/help/it.htm>
- Dept of Treasury: <http://www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml>
- State of CA: <http://www.privacy.ca.gov/cover/identitytheft.htm>
- State of IL:
 - <http://www.obre.state.il.us/FinancialLit/FAQ-IT.htm>
 - <http://www.legis.state.il.us/legislation/legisnet92/hbgroups/hb/920HB5636LV.html>

- <https://www.annualcreditreport.com>
- http://www.aba.com/Consumer+Connection/CNC_contips_idtheft.htm
- <http://www.privacyrights.org/identity.htm>
- <http://www.vaonline.org>
- <http://www.bbbonline.org/idtheft/>
- <http://victimsassistanceofamerica.org>
- <http://www.fraud.org/>
- <http://www.idtheftcenter.org>
- <http://www.llrx.com/features/idtheft.htm>

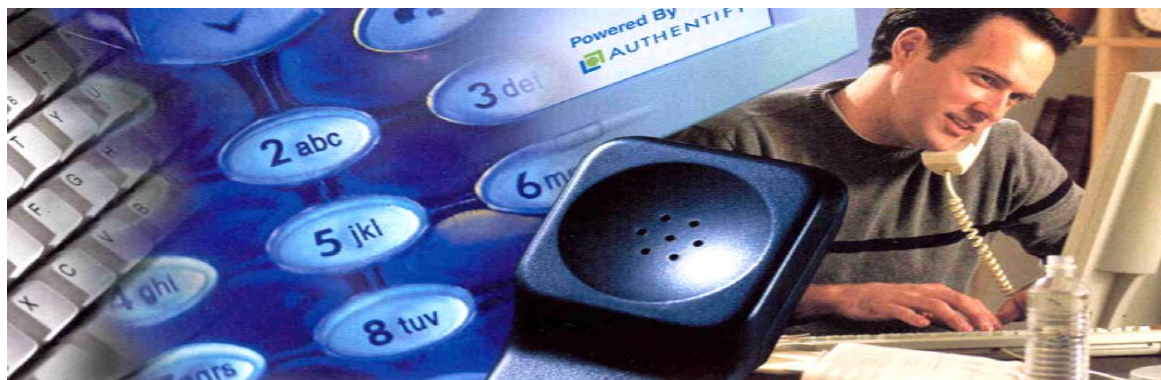
Questions

- Thank you for your time and attention.

*Thanks to the
2004 ACSAC Team!*



Make Contact – Make Certain!



Internet
Identity
Solutions

Contact:

Peter Tapling

773-243-0322

peter.tapling@authentify.com
