LOSING THE PRIVACY WAR

Dr. Margaret Leary, CIPP/G, CISSP, CE|H
Agenda

- Equifax Breach
- Issues with the Use of PII for Identity Authentication
- Recommendations
Equifax Breach Timeline

**March 29 – April 17** - Equifax’s TALX payroll division hacked

**Mid-May, 2017** – Attackers breach Equifax

**July 29** – Equifax discovers breach and stops intrusion

**Aug. 1 and 2** – Three top execs sell of $2 million dollars worth of stock

**Sept. 7th** – disclosed loss of 143 million consumer
Breach included names, SSNs, birthdates, addresses, some driver’s license numbers, and credit card data

**Sept. 8th** – Sen. Warren chastises Equifax for trying to push customers into arbitration

**Oct. 2nd** - Review by Mandiant increased the number affected to 145.5 million – U.S. only databases and about 8,000 Canadians

**Oct. 24th** – UK’s Financial Conduct Authority (FCA) is investigating Equifax for the 400,000, oops....now 694,000 British people affected.
The Technical Details

• Attackers enter through a Web-application, Apache Struts vulnerability, CVE-2017-5638 for which a patch had been released two months prior (granted patch was labor intensive and involved rebuilding all Web apps using the buggy code)

• Equifax had two months to patch, prior to exploitation, and chose not to do so

• Other issues that might have contributed would relate to privilege escalation, or the lack of necessity for the attacker having to even do that. Previously, Brian Krebs had reported that a web portal for handling credit-report disputes in Argentina used admin/admin credentials
Counting the Cost: Profit to Equifax

• End result is FTC, SEC, and multiple states will be lining up to fine and prosecute.

• Based on industry averages, likely to cost tens of millions of dollars (Hall, 2017).

• Equifax loses 143 million records, and provides free credit monitoring services for 12 months.

• But….wait….Equifax sells credit monitoring services ($29.95). How much will it really cost them to provide their own service, TrustedID Premier, for a year “for free”? 

• How many of these subscribers will, then, renew their subscription services at the end of the period?!?

• If only 1% of victims (1.43 million) subscribe after the initial free year that represents - $42.8 million per month - $514 million dollars per year.
The **REAL** Issue

• Did Equifax really do identity management a favor by releasing this information?

• How will a Federal Breach Notification bill inadvertently benefit data aggregators, who are the majority of the lobbyists behind asking for a Federal Bill?

• At stake is a “KBA” (Knowledge-Based Authentication) industry worth billions of dollars
Knowledge-Based Authentication (KBA)

- Authentication protocol that uses security questions based on data aggregated from the individual including:
  - Favorite teacher?
  - SSN
  - DOB
  - Name of first pet?
  - Who holds your mortgage?
  - How much did you finance your car?
  - Square footage of your house?
  - Mothers maiden name

- Service providers (Axiom, Equifax, LexisNexus, Experian, etc.) provide KBA services to all businesses, state, and federal agencies, including to VitalCheck for Birth Certs (“Breeder Docs”)

*Identity attributes in red are those that were lost in the Equifax breach*
The Issues with KBA (Pseudosecrets)

• **Never intended that this information be kept private!!!**
• Social Media Sites
• Guessable
• Discoverable
• Hacked!!
  • Yahoo! Breach in 2013 (revealed in 2016) lost more than 1 billion+ user accounts – including security questions and answers
  • In 2015, hackers accessed IRS’ Get Transcript program (SSNs, etc), which used KBA, to download income tax returns and file fraudulent returns
• NIST even no longer allows its use as an authentication protocol with Federal agencies.......unfortunately, it is still used to authenticate identity to online applications for credit, **which commoditizes these pseudosecrets.**
Discoverability of Pseudosecrets

• My 2008 study analyzed 6,598 public records sites containing identity attributes to determine the frequency with which they can be discovered in public records, calculating a “discoverability index”

• Property records yielded the greatest number of identity attributes, followed by arrest records (including physical attributes and photos), then court records.

• Results confirmed a moderate correlation between FTC-reported ID theft rates and the numbers of public records/contents published by state (some counties publish birth certs of living individuals with mother’s maiden name).
### Comparative Discoverability of Identity Attributes from Online Public Records (not Social Media)

<table>
<thead>
<tr>
<th>Identity Attribute</th>
<th>Index</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>.30</td>
</tr>
<tr>
<td>Home Address</td>
<td>.17</td>
</tr>
<tr>
<td>DOB</td>
<td>.14</td>
</tr>
<tr>
<td>Physical description</td>
<td>.08</td>
</tr>
<tr>
<td>Property value</td>
<td>.08</td>
</tr>
<tr>
<td>Property tax</td>
<td>.08</td>
</tr>
<tr>
<td>Square footage of residence</td>
<td>.08</td>
</tr>
<tr>
<td>Place of Birth</td>
<td>.02</td>
</tr>
<tr>
<td>Birth Year</td>
<td>.02</td>
</tr>
<tr>
<td>Driver’s License Number</td>
<td>.01</td>
</tr>
<tr>
<td>VIN</td>
<td>.01</td>
</tr>
<tr>
<td>Home phone number</td>
<td>.01</td>
</tr>
<tr>
<td>Mother’s Maiden Name</td>
<td>.01</td>
</tr>
</tbody>
</table>
Discoverability

• **Question:** If I posted a file of Social Security Numbers on my Web site (let’s say, ten or twenty thousand of them), have I committed a crime or can this lead to identity theft?
Discoverability

• **Question:** If I posted a file of Social Security Numbers on my Web site (let’s say, ten or twenty thousand of them), have I committed a crime or can this lead to identity theft?

  • No….its just list of numbers. PII is personal data that uniquely **identifies** an individual.
Identity Data Aggregation

• Daniel Solove long ago described a problem with data aggregation where, in isolation, a piece of information may not be invasive, but when amassed, the form a “digital dossier” on the victim (Solove, 2003)

• Using public records, I’ve compiled dossiers including VIN, DOB, name, address, house value, allowing me to calculate DTI and, hence, likely salary within 10 minutes
The Problem with Aggregation

Correlating Discoverable Attributes to Identity Theft Rates

• According to FTC, tax-related fraud (34%) was the most common reported form of identity theft, followed by credit card fraud (33%), phone or utilities fraud (13%), and bank fraud (12%)

• Previous study results (Leary, 2008) demonstrated that states publishing greater numbers of public records tended to have higher identity theft rates

• Ten (67%) of the states with the highest ID theft rates in 2017, were in the top 15 in 2008 (in red)

• Identity theft complaints actually dropped 3% from 2015 – 2016 – however we are talking a drop from 3,140,803 to 3,050,374

• 2017 States with the highest rates included:

  1. Michigan
  2. Florida
  3. Delaware
  4. California
  5. Illinois
  6. Connecticut
  7. Maryland
  8. Missouri
  9. Nevada
  10. Arizona
  11. Georgia
  12. Texas
  13. Rhode Island
  14. Washington
  15. Colorado
So How Privacy Savvy Are You?

• Do you provide “real” information for shoppers loyalty cards, such as at Food Lion or Safeway?
• Do you provide your real SSN at doctor’s offices (is it required to do so)?
• Do you provide your kids’ real SSNs at their schools? Is it required?
• Do you answer authentication questions truthfully at a Website, so you can recover a lost password?
• Do you use a free online service (Gmail, Facebook, etc.)?
• Which is safer, shopping online, or eating out at a restaurant and paying with your credit card?
“All users of email must necessarily expect that their emails will be subject to automated processing. Just as a sender of a letter to a business colleague cannot be surprised that the recipient’s assistant opens the letter, people who use web-based email today cannot be surprised if their emails are processed by the recipient’s [email provider] in the course of delivery. Indeed, ‘a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.”

Google Court Filing  August 2013  - Mick, Jason, 2013. “Google: Yes, we “Read” Your Gmail”

• Feeling glad that you aren’t one of the 425 million Gmail users? Don’t be – have you sent an email to a Gmail user?
Facebook

• Facebook’s Terms of Use specifies that, while you “own” all content and information you post, you grant them a non-exclusive, transferable, sub-licensable, worldwide license to use all IP content that you post on or in connection with Facebook.

• U.S. courts have confirmed that if the data is voluntarily shared with another then it can be posted publicly.

• Important for people to understand that even privatized information on Facebook is collected and sold by Facebook to their business partners and to Federal Agencies.
Who Collects Your PII?

- When surveyed, companies state that your data is their most valuable asset!
- 2010: Axiom stated they had more than 32 billion data records
- Banks and credit card companies
- Retail store owners who sell sales records
- Smart TVs
- Location data with IoT
- Barbies (Hello Barbie)
- Smart Phones
- Your clothes (formerly “spychips”, now inventory tags)
- RFID Chips in people?

Flat Orb advertises that it tracks your product AND your staff.
Who Purchases These Services?

• Banks! (20 – 40% of login services purchased from data aggregators) (Brainard, 2017)

• Credit card companies

• Scammers

• Federal Government, circumventing Privacy Act of 1974 and other OMB Memorandum restrictions on the collection of PII from citizens

• In 2013, the Senate Commerce Committee reported that of nine data aggregator companies investigated, three refused to divulge their data sources and one, Experian, also refused to name its customers.
So What About Breach Notification Laws?

• Immediately following the Equifax breach multiple members of Congress push for a Federal Breach Notification bill. **But will that resolve the problem?**

• There are **NO** federal laws governing the breach of PII (thank heavens)

• There are 48 different state laws (Alabama and South Dakota do not)

• There are regulations (i.e. HIPAA) governing certain industries

• FTC is the largest privacy enforcement agency for consumers
So Is All Lost?

• Won’t resolve until we quit using pseudosecrets to grant instant credit, removing the financial incentive for the commoditization of personally-identifiable information.

• Identity-proofing standards need to be changed – “identity” needs to be assigned at birth (i.e. as with India, which has one of the world’s largest biometric databases of iris’ fingerprint scans of citizens)

• NEC has developed a fingerprint scanner for babies 6 months or older with 99% accuracy
So What Can We Do?

• Lies, lies, and more lies:
  • Do not provide “real” answers to secrets at Websites
  • Do not provide your “real” SSN unless required to do so by the IRS or SSA (or if you are applying for credit)
  • Do not provide “real” information when applying for shopper loyalty cards
  • Do not submit warranties
End User Licensing Agreement (EULA)

Don’t Lock Your Credit - Freeze Your Credit!

• Credit monitoring is worthless, in as much as it is reactive, not proactive.
• Freeze your credit at all three reporting bureaus:
  • http://freeze.Equifax.com
  • https://www.experian.com/freeze/center.html
  • https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp?_ga=2.162593972.943287138.1508890153-1213262464.1508890153
• Usually costs a small fee (up to $20) at each bureau
• Understand that these companies will attempt to steer you/scare you away from freezing your credit, as having access to your data to sell to others is how they make their living
References


