The *EQUIFAX* Experience

What Happened and Where We Are

By Charles Zelhart

Equifax and Its Marketplace

- Ordinary people are ***not*** the customer – we are just a marketable product
- Equifax, Experian, and TransUnion collect **4.5 BILLION** pieces of data *each month*
- Records include addresses, SS numbers, driver's license numbers, utility accts,.....
- The records on an individual, across dozens of databases, typically run to **hundreds** or **thousands** of pages

Equifax – A *Very* Brief History

- Began in Atlanta, GA 1899 as “The Retail Credit Company”
  - Two brothers went door-to-door collecting retail information from grocers and other retailers
  - Compiled the results into a publication called “The Merchants Guide” - $25 annual subscription
  - The company and its competitors spread across the nation employing thousands of investigators
- Reports were widely available for sale.....except..... to the individuals themselves (?!?)

Equifax – A Brief History (Pt. III)

- The strongest agencies continued growing, often through acquisition
- By the late 1990s only the three largest players were left (Experian, Transunion,...& Equifax)
- The agencies discovered and developed a NEW source of revenue...sell the credit reports *back* to the individuals themselves!

Equifax – A Brief History (Pt. II)

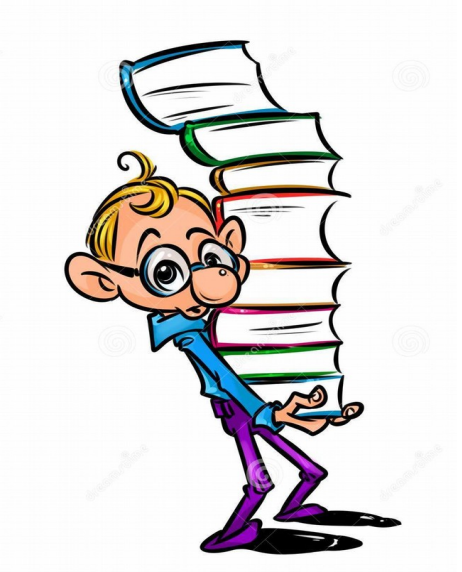
- Impact on citizens' lives continues to grow through the 1960s
- Credit file data used heavily by multiple agencies including the FBI
- Their secrecy and unchecked power finally force Congress to pass legislation in 1970 called the "Fair Credit Reporting Act"

Equifax – A Brief History (Pt. IV)

- In 2001 Equifax teams up with “Fair Isaac” to let consumers buy their FICO scores; the consumer business soon yields $400M/year
- In 2005, Richard F. Smith is hired as the CEO
  - Persuaded more than 7,000 employers to hand over salary details on nearly half the workforce
  - DOUBLED revenue by focusing primarily on new products and revenue growth

Equifax – A Brief History (Pt. V)

- In 2007 Equifax acquires human resources firm “Talx” giving visibility to 142M employment records (300M by 2017...wow...)



- In 2016, initiated a system that paired up consumers' public tweets about their plans and interests with customer (seller) offerings, launching a NEW revenue source!

Equifax – The Woe Begins

- Equifax' size and growth may have fostered a false sense of security. “We've been blessed in our rich history to never have a major breach,” stated newly hired CEO Richard F. Smith at a financial conference in 2005...
- But corp. culture shifted to increasing profit per former VP David Galas, who left in 2011, after 13 years. “It was run a little more like a sports team...you immediately had to get out there and perform...if you didn't, you were cut....”

Equifax – The Woe Grows

- Equifax, Experian, & TransUnion – March, 2013
  - All three agencies acknowledge system intrusions
  - Targets were high profile individuals, including Michelle Obama, Paris Hilton, Hillary Clinton, and Robert Mueller....
- Access was gained w/o use of malware or software vulnerabilities, instead "...leveraging publicly available information to bypass the bureaus' authentication measures by answering all the necessary security questions...."

Equifax – The Woe Grows Pt. II

- Equifax – May 2016
  - Hackers accessed Equifax's W2Express site, which offers downloadable W2 forms
  - Hackers then stole Kroger employees' SSNs & birth dates from other sources and used the information to access the employees' W2 forms
  - Hackers then exposed employees' tax and salary information

- Equifax – March 2017 (not reported until July)
  - API linking bank servers to Equifax breached via stolen credentials?
  - Claimed as unrelated to later exploit

Equifax – The Big “Uh Oh!” Woe

- The “Big Breach...”
  - Happened May 2017 (or ...March 13, 2017?)
  - Discovered July 2017
  - Reported September 2017 (*WHAT ???)*
- Per CEO Richard Smith's written testimony:
  - Equifax sent out an internal email March 9th to deploy the Apache Struts patch within 48 hrs.
  - System failed to identify any vulnerabilities
  - IT dept. included *225 cybersecurity* members who then ran scans that *also* failed to recognize the vulnerability

Equifax – The “Uh Oh!” Woe Pt. II

- Breach attributed to an unpatched flaw, reportedly in Apache “Struts”
  - Struts is a widely-used open source framework for developing and deploying Java-based apps
  - Struts is often deeply embedded in other apps
  - Vulnerability reported as CVE-2017-5638

- Flaw was responsible for “a high number” of exploits in March, 2017 per multiple security firms
- Patch issued March 6, 2017

Equifax – The “Uh Oh!” Woe Pt. III

- Flaw reportedly the “Jakarta” parser (pre 2.5.10.1)
  - Jakarta incorrectly parsed hackers' invalid content-type HTTP header through inappropriate exception handling and error message generation
  - If content-type is invalid (unexpected value type) an error message is triggered
  - Vulnerability occurs because the content-type is not “escaped” following the error
- Situation used by the function “LocalizedTextUtilfindText” to build error message

Equifax – The “UhOh!” Woe Pt. IV

- The resulting function will interpret the supplied message; anything within “$(...)” will be treated as an”Object Graph Navigation Library” (OGNL) expression and evaluated as such
- A hacker can leverage these conditions to execute OGNL expressions that in turn execute system commands

Note: HTTP headers allow the client and the server to pass additional information with the request or the response.

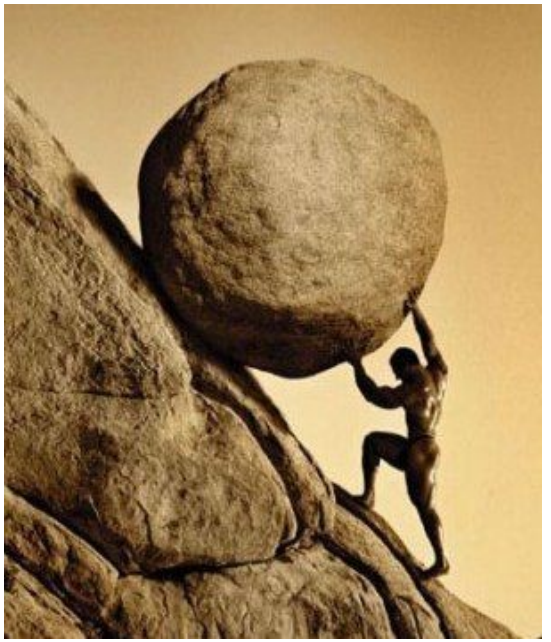
Equifax – A Succinct “Uh Oh” Woe Flaw Description

“The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string.”

(per the *Rapid 7* website)

Equifax – The “Uh Oh!” Woe Dilemma

- Patching the flaw would have been “...labor intensive and difficult....”
- Fix would have required downloading an upgraded version of Struts and then using it to find, replace, and then test – ALL apps that used the existing, buggy versions of the software
- It is possible that Equifax had dozens or even hundreds of such instances spread across multiple platforms in multiple countries



Equifax – The “Uh Oh!” Woe Internal Review

- Per a New York Times – Business Day article of November 9, 2017:
  - The company was continuing to conduct its own internal review of the breach
  - This investigation had already uncovered “two significant deficiencies” in the company's systems that were being remediated
- Blame for the breach was ultimately placed by the CEO on one unnamed individual for failing to address the situation

Equifax – The “Uh Oh!” Woe Impact

- Number of individuals impacted reported as 143M... later raised to 145M+...now 147M+?
- Data exposed appears to have included SSNs, as well as other personally identifiable information such as addresses, driver's license numbers, and similar data...
- The exposure period appears to have been at least 60 days ...and possibly more
- Equifax' response appears to have been limited regarding the the individuals impacted

Equifax – The Company Response

- Company website that was set up was reportedly “...unhelpful and confusing....”
- Company phone lines were reportedly jammed and ineffective
- The site *also* directed users to yet another Equifax product – their “TrustID” credit monitoring product
- The TrustID site *also* included language in its Terms of Service barring those who signed up from suing Equifax – later quietly dropped

Equifax – The Fallout

- Four executives sold company stock worth $1.8M August 1st & 2nd ...prior to disclosure...
  - A company committee cleared the executives
  - Dept. of Justice initiated its own probe of the sales
- CEO, CIO, and the chief security officer all left the company in late September 2017
- Stock price fell from $142.72 (9/07/17) to $92.98 (9/15/17) … but has since recovered to $114.55 (2/13/18)
- Over $87M reportedly spent fixing the flaw (& assoc. costs)

Equifax – The Legal Fallout

- CEO Smith was called to testify before the House Digital Commerce and Consumer Protection Sub-Committee prior to his resignation
- Legislation has been proposed in Congress and the issue of increasing protections for the consumer has received “lip service” ... but no real progress made to date
- Over 240 class action lawsuits have been filed

Equifax – The Legal Fallout Pt. II

- Consumer Financial Protection Bureau, after agreeing to join with the Federal Trade Commission in pursuing the investigation into the Equifax breach, has now stepped back
- 50 State Attorneys General have either initiated action or made formal applications to Equifax for information

The Bureau for Consumer Financial Protection Ruled That....

- Pursuant to section 1028(b) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Bureau of Consumer Financial Protection (Bureau) is issuing this final rule to regulate arbitration agreements in contracts for specified consumer financial product and services. First, the final rule prohibits covered providers of certain consumer financial products and services from using an agreement with a consumer that provides for arbitration of any future dispute between the parties to bar the consumer from filing or participating in a class action concerning the covered consumer financial product or service. Second, the final rule requires covered providers that are involved in an arbitration pursuant to a pre-dispute arbitration agreement to submit specified arbitral records to the Bureau and also to submit specified court records. The Bureau is also adopting official interpretations to the regulation. Effective 9/18/17

...in plain English...firms such as Equifax *cannot* bar consumers from suing such firms, even if they have arbitration agreements....BUT...

...Congress Negated It....

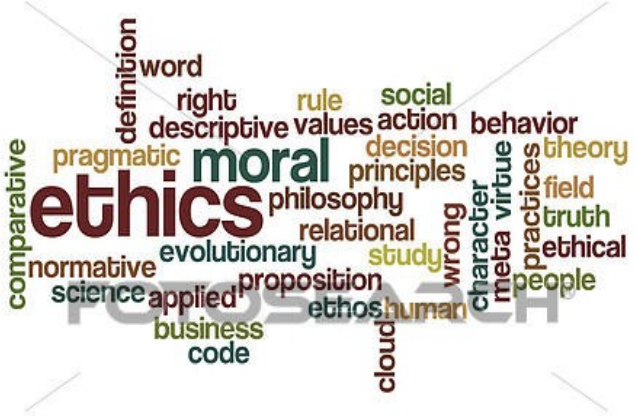
- The *day after* the above ruling was issued by the Bureau for Consumer Financial Protection Congress voted to override it
- The House voted 231 to 190, along party lines
- The Senate split 50-50, with Senators John Neeley and Lindsay Graham joining the Democrats - the tie was broken by the Vice President
- While Congress has passed legislation, the ultimate impact is still open to question

Equifax - Ethical Points

- Equifax considers the consumer to be product for sale rather than an individual
- Equifax failed to take the steps necessary to safeguard consumers' information
- Equifax failed to publicly announce the breach for over 6 weeks...and possibly as long as long as 6 months
- Equifax failed to accurately assess the full extent of the breach...twice

Equifax – Ethical Points Pt. II

- Equifax allowed executives to sell their stock around the time the breach was announced
- Equifax convened a committee that cleared these executives of any wrongdoing...but the investigation was purely internal
- Equifax initially included terms that required consumers to give up their right to sue if they took advantage of Equifax' vulnerability scan



Equifax – Ethical Points Pt. III

- Equifax exploited the situation by using it to market yet more products & services to consumers
- Congress “muddied the water” by immediately passing legislation to negate a decision by the Bureau for Consumer Financial Protection that would have given the consumer some chance for redress through legal recourse...not just an ethical question but a Constitutional one.....

Feeling Comfy Now???

So...What Can You Do?

- Find out if your information may have been exposed
  - Equifax is offering this service for free but can you trust them after what has already happened?
  - Experian has also jumped into this arena
- Consider enrolling in a credit monitoring program
- Contact the credit reporting companies and request a report from each

What Can You Do? Pt. II

- Monitor your accounts for unusual activity
- Consider setting a fraud alert on your credit accounts...fairly easy to do but does NOT block new credit being extended
- Consider placing a credit freeze on your credit accounts.....HOWEVER, you MUST make sure to retain and safeguard the access code they issue to you!

Questions?

Sources

Apache Struts Jakarta - Multipart Parser OGNL Injection – Metasploit Exploit Database 3/15/17

How Hackers Broke Equifax: Exploiting A Patchable Vulnerability – Forbes 9/14/17

Failure to patch two-month-old bug led to massive Equifax breach – Arstechnica September, 2017

Former Equifax CEO says breach boiled down to one person not doing their job – Techcrunch 10/03/17

As Equifax Amassed Ever More Data, Safety Was a Sales Pitch – New York Time 9/23/17

Equifax hack put more info at risk than consumers knew – ABC News2/09/18

Equifax faces hundreds of class-action lawsuits and an SEC subpoena over the way it handled its data breach - Hayley Tsukayama Washington Post 11/09/17

Equifax now hit with a rare 50-state class-action lawsuit - Tara Swaminatha CSO 11/22/17

Congress votes to disallow consumers from suing Equifax and other companies with arbitration agreements - Devin Coldewey TechCrunch 10/24/17

Equifax faces class action lawsuit - Eric Mandel Atlanta Business Chronicle 11/27/17

Equifax Faces Mounting Costs and Investigations From Breach - Stacy Cowley NY Times-Business Day 11/09/17

Sources (cont'd)

4 Credit Bureau Data Breaches that Predate the 2017 Equifax Hack – David Bisson, Tripwire 9/14/17

Equifax suffered another data breach in March - Hamza Shaban Washington Post 9/18/17

CVE-2017-5638: Anatomy of the Apache Struts Vulnerability – Stephen Mort BlackDuck 9/14/17

After Equifax Hack, Consumers Are On Their Own. Here Are 6 Tips To Protect Your Data - Yuki Noguchi NPR Business 9/14/17

Prepared by Charles Zelhart