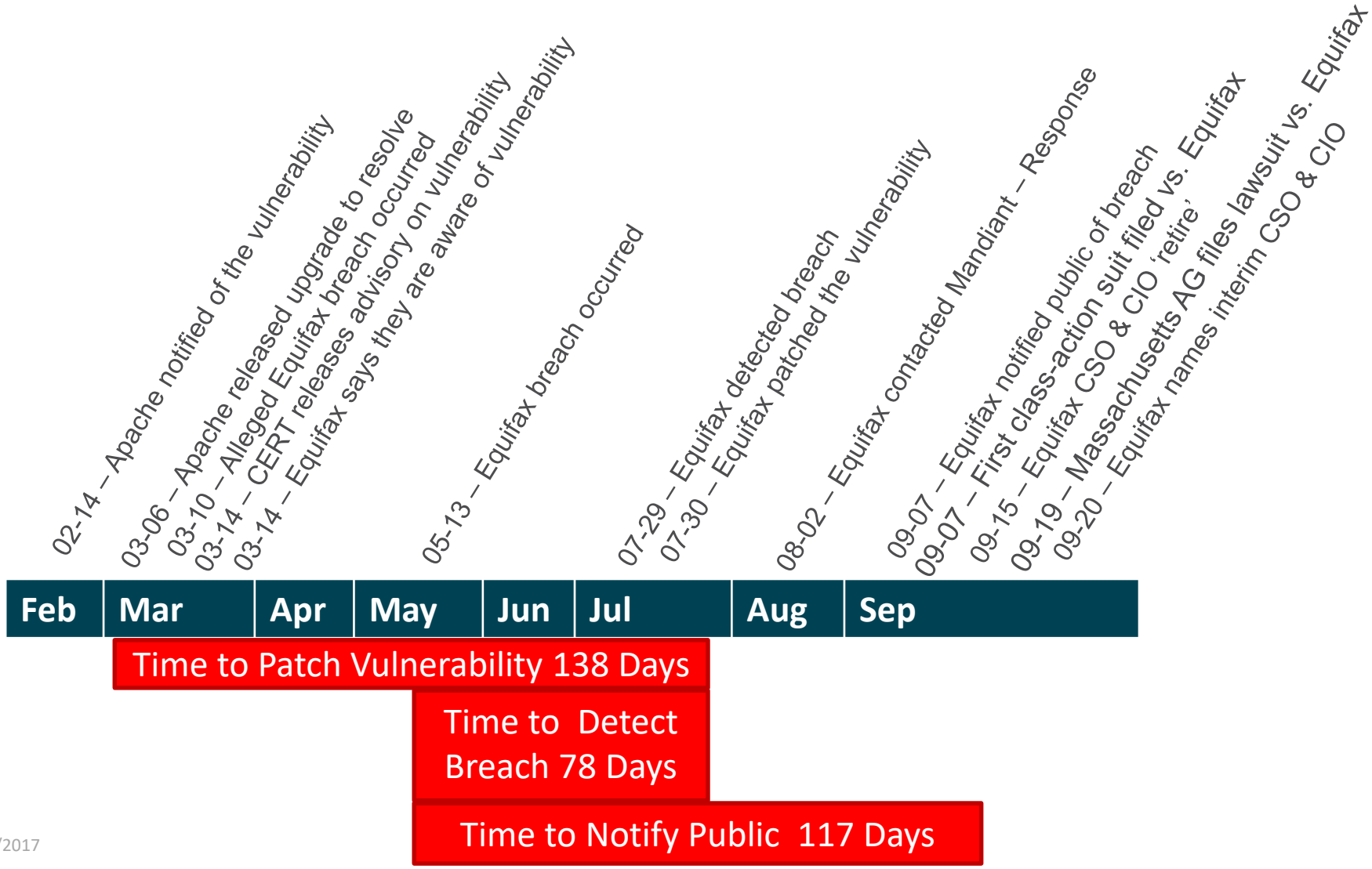
The Equifax Breach and Credit Union Involvement

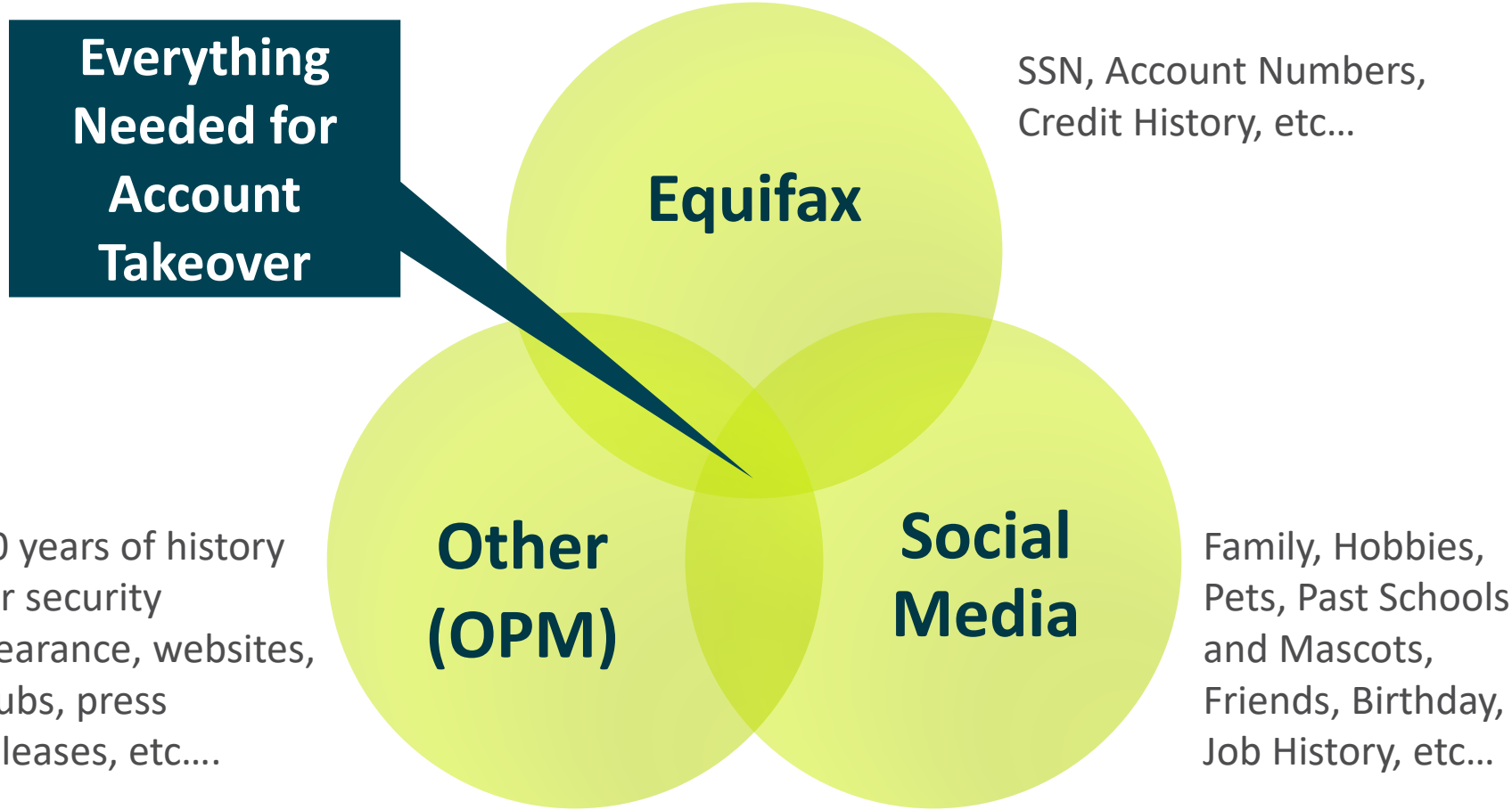
Gene Fredriksen CISM,CRISC

Equifax Information Overload

Equifax Timeline



The Additive Effect – No Breach is Stand Alone….



Equifax: A Great Team That Forgot Basic Blocking and Tackling

- Equifax used the Apache Struts web-application software
- Vulnerability was disclosed in March. There were clear and simple instructions of how to patch
- Equifax had ample opportunity to update.
- Equifax was attacked in May, leveraging an unpatched system
- Had they patched, the breach would not have occurred

Patching Isn't Sexy, But It Is Always Critical

Challenge at the Credit Union:

Smaller Staffs and Conflicting Priorities

Vulnerability Details : CVE-2017-5638

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

CVSS Scores & Vulnerability Types CVSS Score **10.0 Critical**

Vulnerability Type	Rank	Description
Confidentiality Impact	Complete	There is total information disclosure, resulting in all system files being revealed.
Integrity Impact	Complete	A complete loss of system protection, resulting in the entire system being compromised.
Availability Impact	Complete	The attacker can render the resource completely unavailable.
Access Complexity	Low	Very little knowledge or skill is required to exploit.
Authentication	Not Required	Authentication is not required to exploit the vulnerability

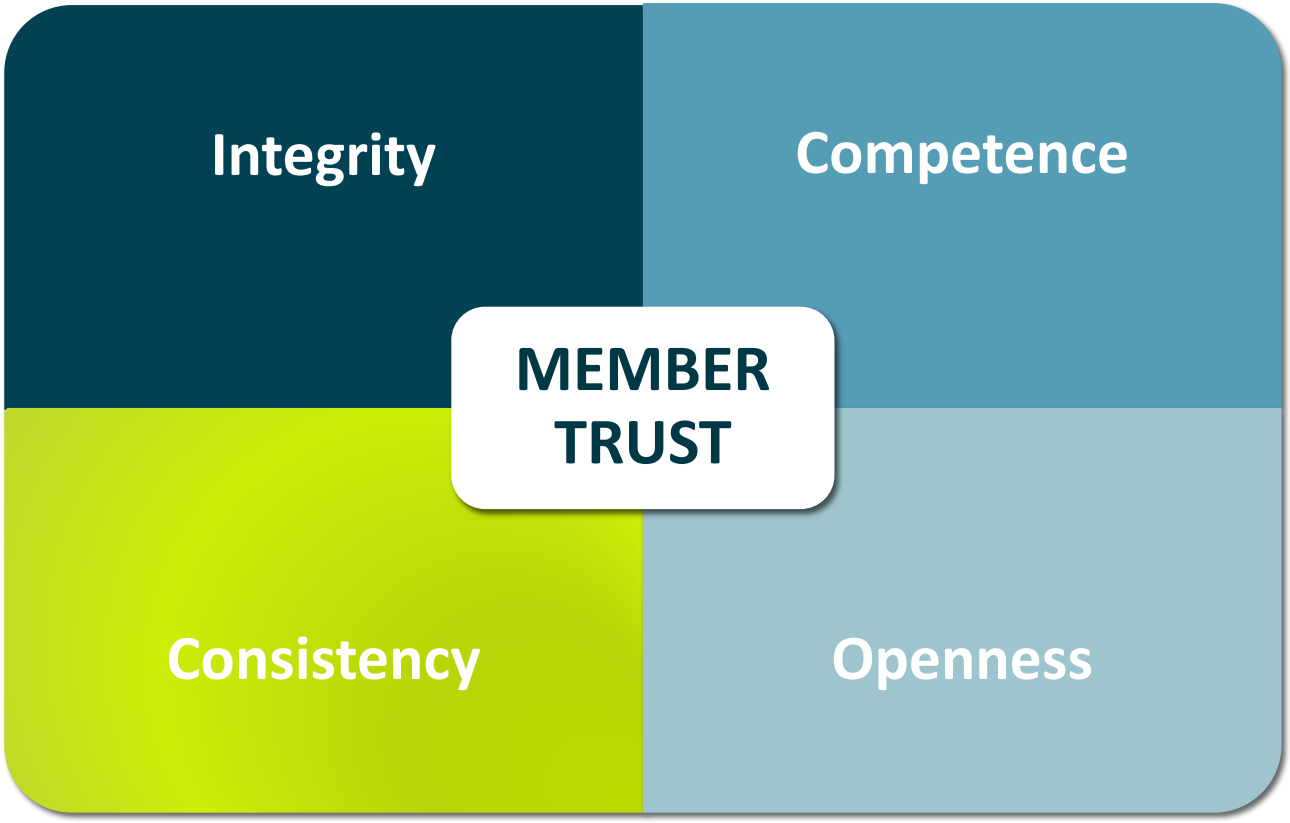
Public Notification – What's Good

- Demonstrate true, unquestionable, care and concern.
- Inform, address and answer, the key concerns of their stakeholders.
- Communicate consistently across all channels, groups and regions.
- Communicate in plain English, not using corporate or legal talk.
- Comply with appropriate jurisdictional laws and regulations concerning breached PII.

Lessons from the Equifax Announcements

- Should have used stronger language to show that they *knew* that this breach was unacceptable
- Should have admitted that they violated customer trust
- Stated they are committed to doing anything and everything to help impacted consumers protect themselves.

Goal: Maintain Member Trust



Everyone fails to meet expectations at some point. You will be judged by others on what you do and how you respond

Fraud: Increased Synthetic Fraud?

- The Equifax breach's theft of personally identifying information is a game-changer for fraud and authentication.
- Synthetic Fraud – will get an especially huge boost

- **Fake profiles:** real information with a few minor changes
- **Applies for loan:** rejected - no exact match in the system
- Action creates a credit file on the fake applicant
- Criminal then applies for low limit credit card. That lender will check the credit, find that new credit file and issue the card
- That builds credit history for a fictitious person, and the criminal can continue borrowing under the fictional profile

Potential Regulatory Oversight

- Federal laws give the CFPB the power to supervise and examine large credit-reporting firms to ensure the quality of information they provide.
- CFPB called for expanded powers to cover data security to prevent breaches and suggested placing monitors inside credit reporting firms, borrowing a tactic from the regulatory regime for banks.
- PCI Regulations, FFIEC, NCUA
- Vendor oversight and management

Legislation

- Sen Markey (D-Mass) introduced legislation Thursday that would press data broker companies, to implement better privacy and security practices.
- The bill, co-sponsored by Sens. Richard Blumenthal (D-Conn.), Al Franken (D-Minn.) and Sheldon Whitehouse (D-R.I.), would mandate "comprehensive" privacy and security programs at data brokers and allow the public to opt out of having their data included in data sales. The FTC would be in charge of enforcement.

Legislation

H.R. 3806 Rep Langevin (D)

- To establish a national data breach notification standard, and for other purposes.
- “any business entity engaged in or affecting interstate commerce, that uses, accesses, transmits, stores, disposes of, or collects sensitive personally identifiable information about more than 10,000 individuals during any 12-month period shall, following the discovery of a security breach of such information, notify, in accordance with sections 4 and 5, any individual whose sensitive personally identifiable information has been, or is reasonably believed to have been, accessed or acquired.”

Legislation

S.1816 Sen Warren (D-MA)

Freedom from Equifax Exploitation Act

- To amend the Fair Credit Reporting Act to enhance fraud alert procedures and provide free access to credit freezes, and for other purposes.
- not later than 1 business day after receiving the request sent by postal mail, toll-free telephone, or secure electronic means as established by the agency, place a credit freeze on the file of the consumer
- not later than 15 minutes after receiving the request by toll-free telephone number or secure electronic means established by the agency, if the request is received during regular business hours…..

Vendor Management Responsibilities

- **Vendor Details**—who they are, who owns them, where are they located, the basics.
- **Reputation**—do their customers like them, do they provide the right service, are there any red flags your institution will suffer by entering into a relationship with said vendor.
- **Financial Stability**—are they profitable enough to provide your critical services for the life of the agreement and expected use of the service.
- **Cybersecurity**—are your institution's data and transactions safe on the vendor's systems?
- Mandate SLA's for suspected breach and breach notification.

Equifax Security Program Lessons for Credit Unions

Lesson	Comment
Assume you are already hacked. At all times.	Build operations and defense with this premise in mind.
The root cause of the breach was a website vulnerability but the data lived on the endpoint.	Secure the DATA not just the network.
Detection still takes too long.	1 day is too long for an attacker to be in your system.
Visibility remains the key to detection and prevention.	You cannot detect what you cannot see.
We are all in this together.	Data is linked. One breach can be leveraged for the next or the next.
It doesn't matter how big you are.	Equifax has a 225 person security staff.
Encryption is your friend.	These efforts aren't simple and take time, but the benefits outweigh risks.
Secure vendor connections	You are responsible.

Questions Credit Union Boards Should Ask

- Does your organization have a documented, robust patching practice?
- Is your organization comprehensive, thorough and disciplined with respect to the risk and vulnerability assessment, penetration testing of the organization and mission-critical systems and applications.
- Does your organization have efficiently implemented layers of security control?
- Is your security strong enough to resist a single vulnerability compromising members information?
- Do you have encryption of such sensitive information so as to protect them even if the system is hacked?

Questions

Gene Fredriksen
gfredriksen@pscu.com


PSCU