RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: LAB4-R10

Everything You Need to Know About Cybersecurity & Privacy Law in 2 hours!

Dr. Chris Pierson
CEO
BLACKCLOAK
@BlackCloakCyber

James T. Shreve
Partner
Thompson Coburn
@ThompsonCoburn

Agenda

- 2 Hours
- Privacy & Cybersecurity Laws
  - Safeguarding Laws
  - Hacking Data Breach Laws
  - Privacy Laws
- 3 Scenarios

Rules

- Chatham House Rule:
  - "Participants are free to use the information received, but neither the identity nor the affiliation of the speaker(s), nor that of any other participant, may be revealed"

RSAConference2019

Part I. Safeguarding Laws

FTC Act & UDAP

Name: Federal Trade Commission Act / Unfair or Deceptive Acts or Practices (Section 5)	1914
Applies to: All organizations engaged in interstate commerce	Federal & State 15 USC § 45
Summary: This law prohibits the use of "[u]nfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce." The FTC has determined certain privacy practices to be unfair methods of competition or deceptive acts under the Act. Such as, an organization's: • Violation of its own privacy policies and promises, • Use of spyware and adware, and • Failure to secure sensitive consumer information. CFPB also has authority to prohibit abusive acts.	Civil
Penalties: $10,000 in fines per violation	
Enforcement: FTC, CFPB	

SEC Cybersecurity Guidance

Name: CF Disclosure Guidance: Topic No. 2 - Cybersecurity **Commission Statement and Guidance on Public Company Cybersecurity Disclosures**	2011 2018
Applies to: All Public Companies	Federal
Summary: This SEC Disclosure Guidance mandates that all public companies include in quarterly and annual public filings information on cyber risks and threats to systems and business operations. Threats may include vulnerability to hacking, potential lawsuits, or potential reputational damage. Corporations must evaluate the cyber risks and threats as they pertain to each specific business practices and disclose in filings any risk or threat that are "material." 2018 Updates: (1) disclose Board's role in managing cybersecurity risk, their expertise, and interface with senior management, (2) update incident response procedures to include disclose analysis review, (3) mitigate insider trading risks around the same time, (3) disclose material incidents promptly, and (5) avoid generic disclosures.	SEC Guidance
Penalties: No explicit penalties, but failure to follow can lead to other SEC actions or shareholder suits	
Enforcement: SEC	

GLBA Safeguards

Name: Gramm-Leach-Bliley Act **Federal financial regulators' Safeguards Rule**	1999 2001, 2002
Applies to: Financial Institutions	Federal 15 USC § 6801, 6809
Summary: This law mandates that all covered financial institutions have an information security plan in place that establishes policies and procedures for the protection and security of clients' NPI. The plan should include • At least one designated employee to manage the plan; • A risk analysis covering all threats unique to each department's handling of NPI; and • Monitoring and testing procedures. The safeguards must be updated to reflect current risks as the need arises.	Civil 
Penalties: Up to $250,000 in fines	
Enforcement: CFTC, SEC, FTC, NCUA, FRB, FDIC, OCC, State insurance authorities	

NY DFS Cyber Guidance

Name: Cybersecurity Requirements for Financial Services Companies	2017
Applies to: Covered Entities include banks and other financial service firms - "any Person operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law, the Insurance Law or the Financial Services Law."	23 N.Y.C.R.R. Part 500
Summary: NY Department of Financial Services (DFS) implemented a rule that requires covered entities to adopt and maintain a cybersecurity program and corresponding cybersecurity policies and procedures. Many of the requirements overlap with FFIEC Guidance, GLBA, and other data security laws, but there are a number of differences. Requirements: 1. Maintain a risk-based cybersecurity program and policies & procedures 2. Designate a CISO to oversee the program and deliver an annual written report to management. 3. Implement numerous cybersecurity controls designed to keep NPPI safe (pen testing, 2FA, IAM, encryption) 4. Establish a written security incident response program; notify DFS within 72 hours of a cybersecurity event 5. File annually (by Feb 15, 2018) a written certification of compliance with these requirements **Primary source for NAIC Model Cybersecurity Law**	Civil
Penalties: Numerous types of oversight and civil fines	
Enforcement: New York DFS	

FACTA ID Theft Red Flags Rule

Name: Fair and Accurate Credit Transactions Act (FACTA) Identity Theft Red Flags Rules	2007
Applies to: Institutions with covered financial accounts (all financial accounts – cable, bank, etc.)	Federal
Summary: This law mandates that institutions must: 1. Identify relevant "red flags" for covered accounts to be incorporated into the Program; 2. Detect red flags on covered accounts according to the Program; 3. Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and 4. Ensure the Program is updated periodically to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft. The regulation defines a "Red Flag" as a pattern, practice, or specific activity that indicates a possible risk of identity theft.	Civil 
Penalties: Civil	
Enforcement: FTC, regulatory agencies	

HIPAA/HITECH

Name: Health Insurance Portability and Accountability Act **Health Information Technology for Economic and Clinical Health Act**	1996 2009
Applies to: Covered Entities and, in some cases, Business Associates	Federal
Summary: 3 Key provisions relating to privacy and security (1) The Privacy Rule mandates Covered Entities and Business Associates have safeguards in place to protect the privacy of all Protected Health Information (PHI). PHI includes any payment history for healthcare, provision of healthcare, and past, present or future health conditions. (HIPAA) (2) The Security Rule mandates Covered Entities and Business Associates have administrative, physical, and technical safeguard in place to protect Electronic PHI. (HIPAA) (3) The Breach Notification Rule mandates that all Covered Entities and Business Associates give notification to the media and to individuals affected following a breach of unsecured PHI affecting more than 500 people. (HITECH)	Civil
Penalties: up to $50,000 in fines per violation with a $1,500,000 cap per year.	
Enforcement: HHS (OCR), FTC	

Massachusetts Data Security Regulations

Name: Standards for the Protection of Personal Information of Residents of the Commonwealth (201 CMR 17.00)	2010
Applies to: Persons possessing personal information relating to MA resident	State
Summary: • Any companies or persons who store or use personal information (PI) about a Massachusetts resident develop a written, regularly audited plan to protect personal information. • Both electronic and paper records will need to comply with the new law. • Secure user authentication, secure access control, encryption, monitoring, removable media and mobile devices encrypted, patched computers, up-to-date anti-virus, user education	Civil
Penalties: Civil penalties	
Enforcement: State AG	

Plastic Card Security Acts

Name: Nevada Bill 227 **Minnesota Plastic Card Laws (325E.64)**	2007 2010
Applies to: Certain entities doing business in the state	State
Summary: **Nevada**: required "data collectors" (businesses or government agencies) who are "doing business" in the state and who accept payment cards to comply with the PCI DSS. **Minnesota**: any "person or entity conducting business in Minnesota" is prohibited from storing security codes, PIN numbers, or the full contents of any track of magnetic stripe data from customers' debit or credit cards (collectively, "Protected Customer Data") for more than 48 hours after authorization of a transaction. A business is also responsible under the PCSA if its payment card "service provider" (i.e., a third party that stores, processes or transmits customers' payment card data on behalf the business) stores Protected Consumer Data beyond the 48-hour limit.	Civil
Penalties: Civil penalties to regulated entities	
Enforcement: State AG	

Nevada Encryption

Name: Nevada Personal Information Data Privacy Encryption Law	2009, 2011
Applies to: All Businesses	State Nev. Rev. Stat. § 603A.215
Summary: This law mandates that all business encrypt all electronic personal information to protect from "unauthorized access, acquisition, destruction, use, modification, or disclosure." Defines encryption as the protection of data in electronic or optical form, in storage or in transit, using an encryption technology that has been adopted by an established standards setting body, such as NIST.	Civil
Penalties: Injunction	
Enforcement: State AG	

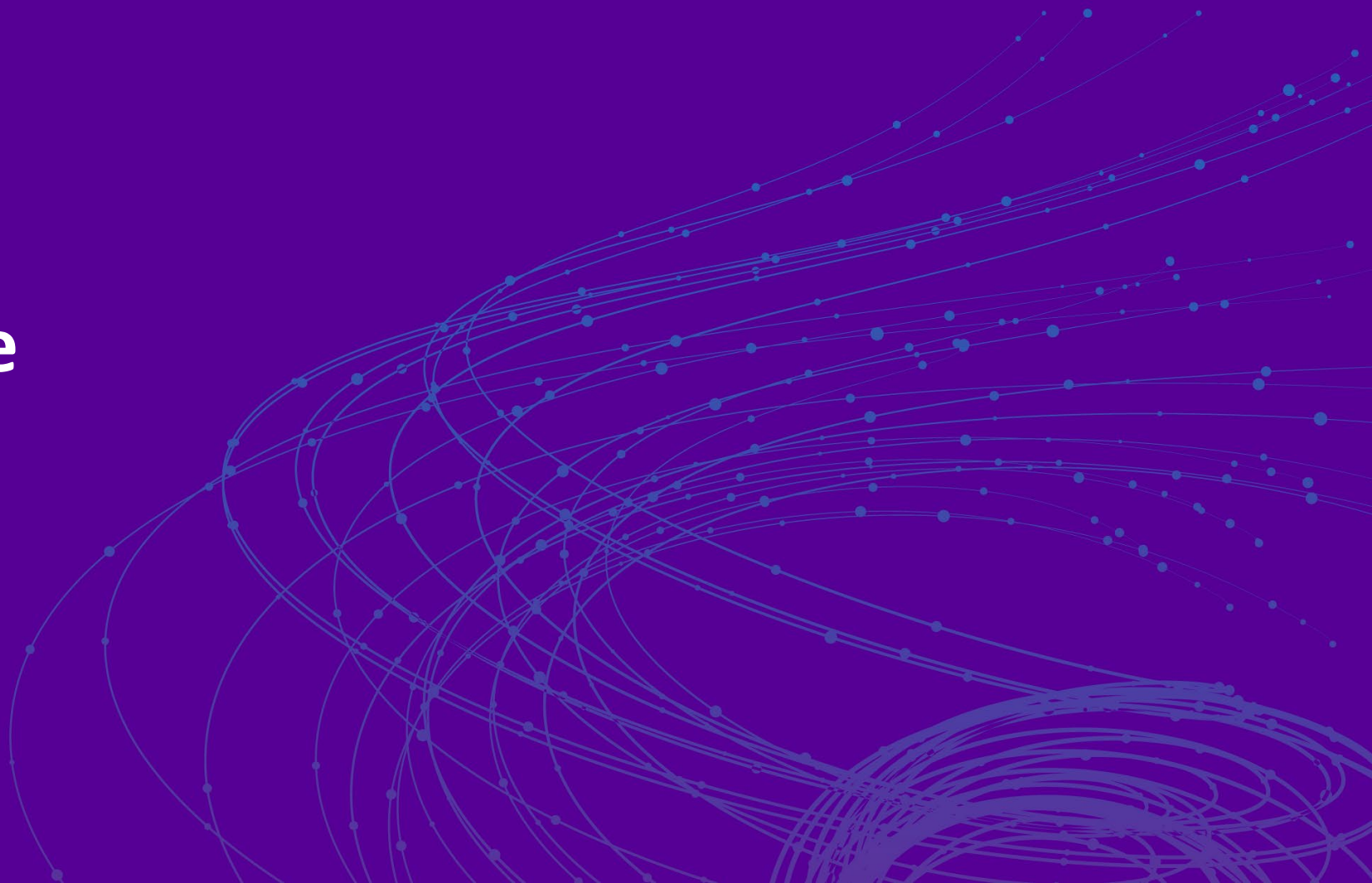
Connecticut SSN Act

Name: Connecticut SSN Act	2008
Applies to: All Connecticut companies or those with minimal contacts to Connecticut	State (CT) Public Act No. 08-167
Summary: Requires businesses that maintain personal information (*e.g. Social Security number (SSN), driver's license* number, account number, or credit/debit card number), to: 1) Safeguard the personal information as well as the computer files and documents containing the information; 2) destroy or make unreadable information prior to disposal; and 3) create and publish a SSN privacy policy (if a company collects SSNs in the course of its business). The policy must protect the SSNs from disclosure, prohibit unlawful disclosure of SSNs, and limit access to SSNs.	Civil 
Penalties: Civil penalties up to $500,000 per incident	
Enforcement: State AG	

RSAConference2019

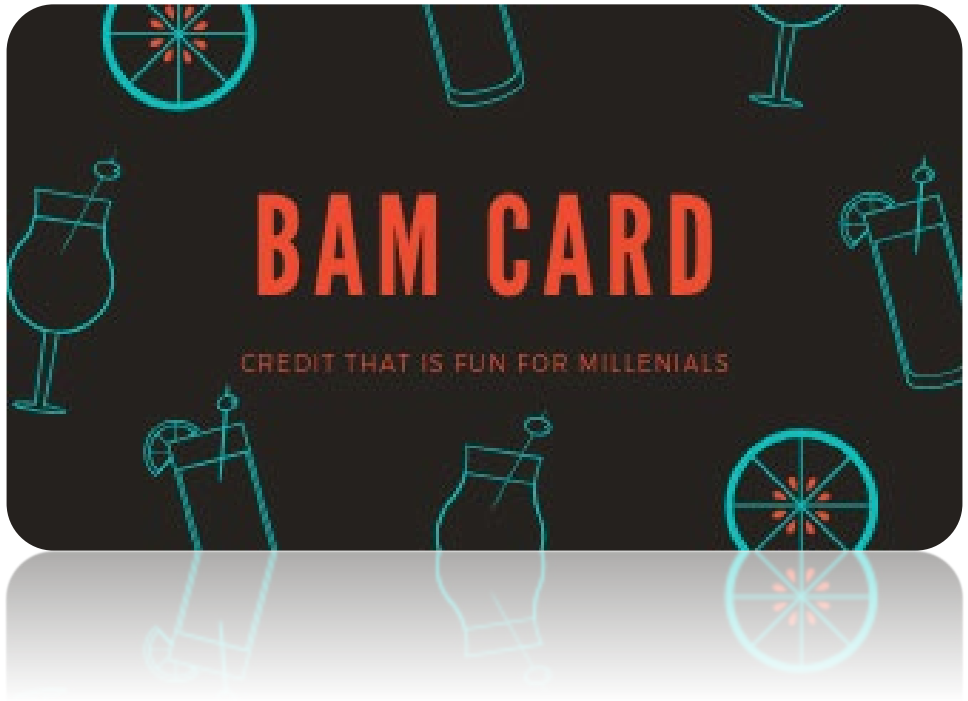
Scenario One

FinTech Oopps



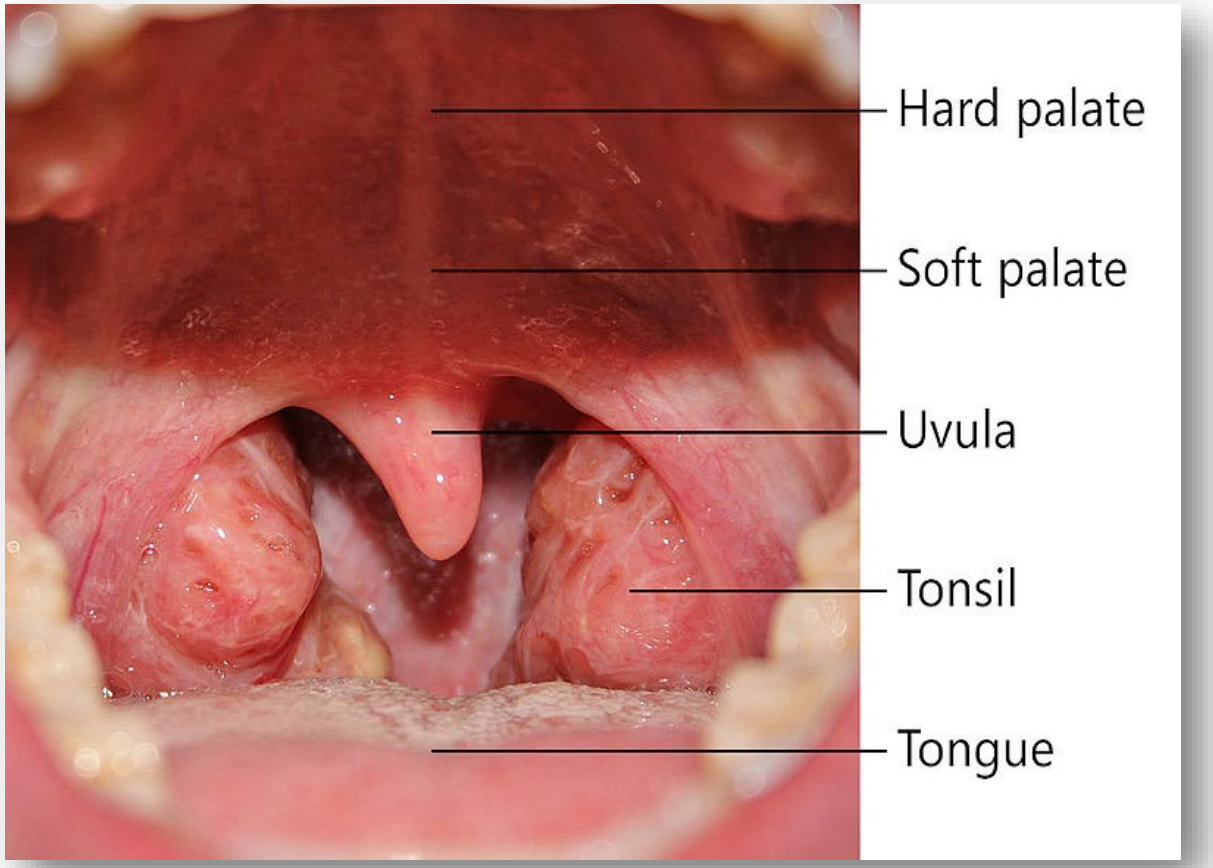
Scenario One

- You are the Head of Payments for the BAM Card - a new credit card that fits the lifestyle of Millennials
- It weights .5 lbs and is pure titanium
- You are looking for cyber talent and heard RSAC is the place to be
- You flew to SFO and after a brisk cocktail or two ended up leaving your laptop on the plane



Scenario One

- Your laptop was not encrypted and its password (since the Dir. of Security makes it so hard) is taped to the bottom.
- On the laptop are:
  - Emails on new hires and their credit reports
  - Test payments and error files from banks on credit card transactions
  - The original BIN file for the first credit card run
  - Cool intellectual property on a new biometric login using customer's uvula's



Scenario One

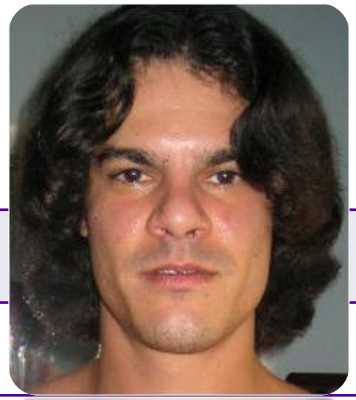
- Also included are:
  - Your company's next SEC quarterly filings (you are public)
  - A few folders on new acquisition targets for your company to purchase
  - Your company's most recent financial audit reports for the NY DFS under your financial license
- Now what?

RSAConference2019

Part II. Hacking/Data Breach Laws

Computer Fraud and Abuse Act (CFAA)

Name: Computer Fraud and Abuse Act (CFAA)	1986
Applies to: All protected computers (i.e. all computers in the US or involved in interstate or foreign commerce anywhere).	Federal 18 USC §1030
Summary: Access the exceeds authorization/Unauthorized Access: Anyone who (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains (A) information contained in a financial record of a financial institution, (B) information from any department or agency of the United States; or (C) information from any protected computer;	Civil & Criminal
Penalties: 5 yrs. criminal penalty, up to $250,000 in fines	
Enforcement: US DOJ, Private Parties	



Electronic Communications Privacy Act (ECPA

Name: Electronic Communications Privacy Act (ECPA)	1986
Applies to: All U.S. Entities and those with Minimal Contacts to the U.S.	Federal 18 USC §§2510-2522
Summary: This law has three parts: • Wiretap Statute protects wire, oral, and electronic private communications while in transit (generally requires a warrant) • Stored Communications Act (18 USC §2701-2712) – prohibiting access to stored communications (> 180 days emails; subpoena) • Pen Register Act (18 USC §§3121-3127) - governing tracing of telephone communications (court order) Other amendments include CALEA, USA PATRIOT Act, and FISA	Civil & Criminal
Penalties: 5 yrs. criminal penalty, up to $250,000 in fines	
Enforcement: US DOJ, Private Parties	

Type of Communication	Required for Law Enforcement Access	Statute
Email in Transit	Warrant	18 U.S.C. § 2516
Email in Storage on Home Computer	Warrant	4th Amendment, US Constitution
Email in Remote Storage, Opened	Subpoena	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for 180 days or less	Warrant	18 U.S.C. § 2703
Email in Remote Storage, Unopened, Stored for more than 180 days	Subpoena	18 U.S.C. § 2703

Foreign Intelligence Surveillance Act (FISA)

Name: Foreign Intelligence Surveillance Act (FISA)	1978
Applies to: U.S. Agencies	Federal 50 USC §1801
Summary: • Creates a legal regime for the surveillance of “foreign intelligence” that is outside of the Wiretap Statute. Allows for the interception and collection of foreign intelligence information (esp. electronic), physical entry, pen-trap/trace, and business records. • Defines "foreign intelligence information" to mean information necessary to protect the United States against actual or potential grave attack, sabotage or international terrorism. • The government must show probable cause that the “target of the surveillance is a foreign power or agent of a foreign power.” • President can request through AG for 1 year; 15 days prior to war; or others can under emergency for 72 hours. • Foreign Intelligence Surveillance Court (FISC); 11 Federal Judges	Civil & Criminal 
Penalties: 5 yrs. criminal penalty, up to $10,000 in fines; civil fines	
Enforcement: US DOJ	

Data Breach requirements

Name: Various	2003 to present
Applies to: Persons owning or possessing personal information relating to state residents	Federal and State
Summary: All 50 states, DC, PR and USVI have enacted laws applying to unauthorized access to personal information, generally but not always in computerized form, relating to state residents. Owners must notify affected residents and, in some states, one or more state agencies. Non-owners must notify the owner. Financial institutions regulated by the federal bank regulatory agencies and entities subject to HIPAA generally are exempted from the state requirements, but have separate federal notice requirements	Civil
Penalties: Varies by state	
Enforcement: State AGs, some private rights of action	

GDPR Data Breach

Name: General Data Protection Regulation Articles 33-34	2018
Applies to: Entities established in the EU or targeting data subjects in the EU or monitoring their activity	EU
Summary: Notice requirements on the data controller Notice to the data protection authority within 72 hours of becoming aware of a personal data breach Notice to data subjects where the incident is likely to result in a high risk to the rights and freedoms of natural persons (with some exceptions)	Civil
Penalties: Fines of up to the greater of 10 million Euros or up to 2% of the entity's global worldwide annual turnover for the prior year	
Enforcement: Data protection authorities	

Canadian Data Breach

Name: Personal Information Protection and Electronic Documents Act (PIPEDA)	2015 (enacted) 2018 (regulation)
Applies to: Entities controlling personal information	Canada
Summary: The law requires notice to the Office of the Privacy Commissioner (OPC) and affected individuals for any breach of security safeguards where it is reasonable to believe the breach creates a real risk of significant harm to an individual. Notice may also be required to law enforcement or other organizations that could reduce the risk of harm for the breach. The regulation also contains recordkeeping requirements for information around breaches and response.	Civil
Penalties: None specified, but the Attorney General can impose fines	
Enforcement: Attorney General of Canada	

RSAConference2019

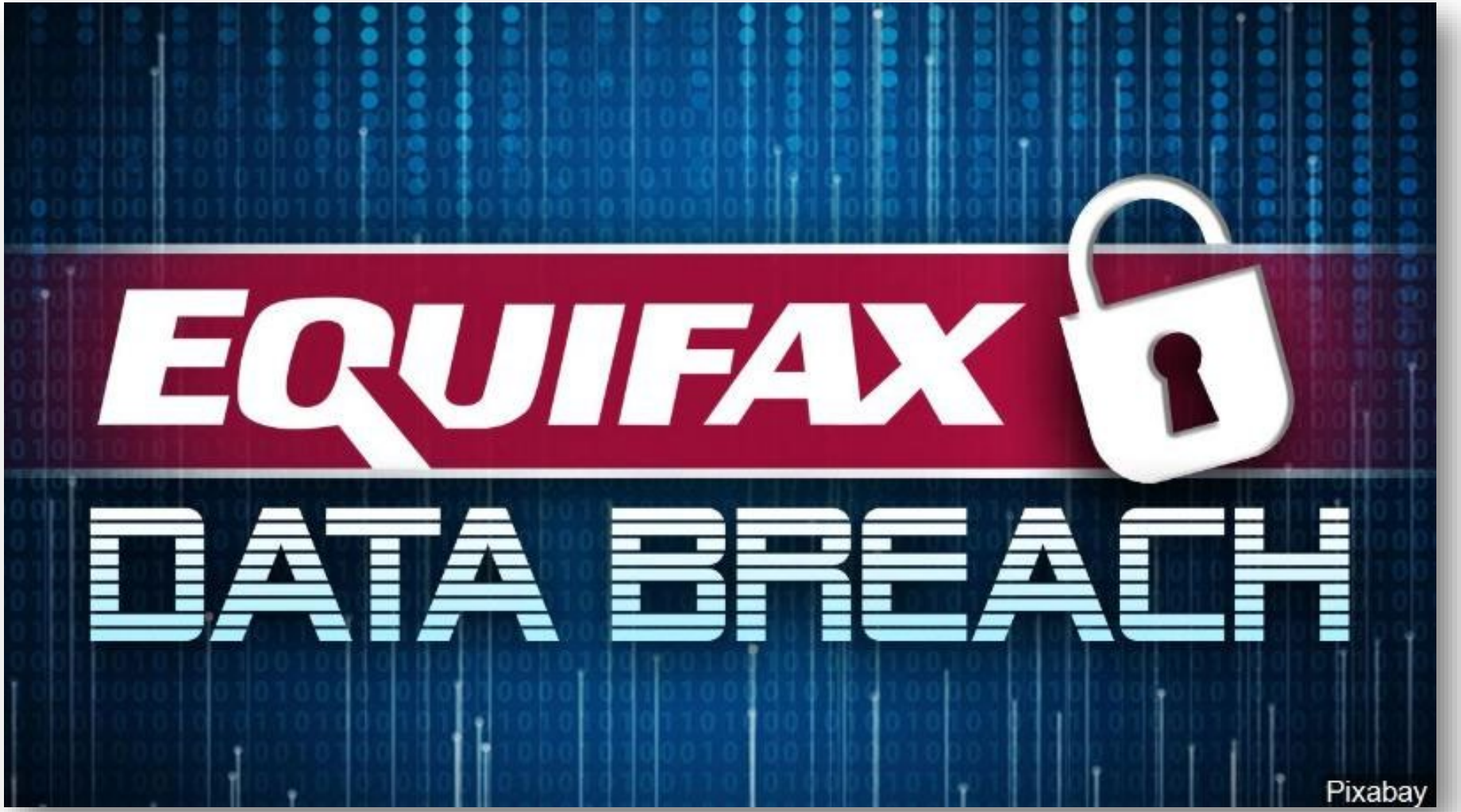
Scenario Two

Data Breach or No Data Breach

Breach or No Breach

Scenario Two

Scenario Two



Scenario Two

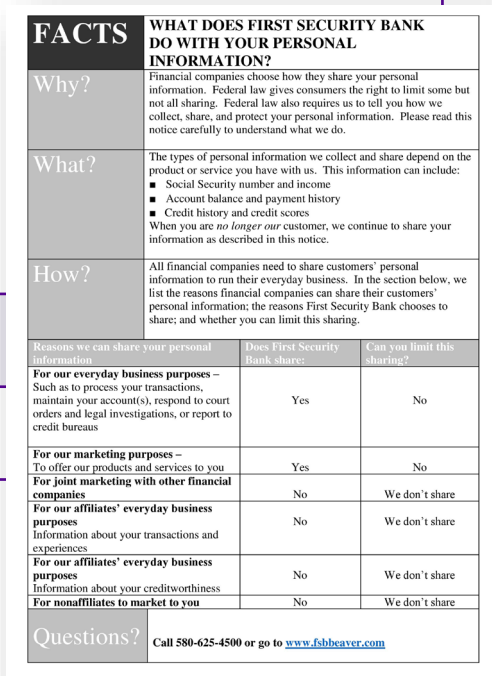
Scenario Two

RSAConference2019

Part III. Privacy Laws

GLBA Privacy

Name: Gramm-Leach-Bliley Act **Privacy Rule**	1999 2000, 2011
Applies to: Financial Institutions	Federal 15 USC § 6802-6809
Summary: • Restricts Financial Institutions' sharing of consumers' and customers' "Nonpublic Personal Information" (NPI) with nonaffiliated third parties. • Mandates that privacy notices be given to consumers and customers disclosing information collection and sharing practices and providing a right to opt-out. Some exemptions apply. • NPI includes any information a consumer provides to obtain a product or service, any consumer information resulting from a transaction, or any other information obtained by providing a product or service.	Civil (theoretically criminal)
Penalties: Potential fines vary by regulator	
Enforcement: CFPB generally, CFTC, SEC, FTC (limited), certain other regulators	



FACTS	WHAT DOES FIRST SECURITY BANK DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ■ Social Security number and income ■ Account balance and payment history ■ Credit history and credit scores When you are *no longer our* customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons First Security Bank chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does First Security Bank share:	Can you limit this sharing?
For our everyday business purposes – Such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	Yes	No
For our marketing purposes – To offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes Information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes Information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	**Call 580-625-4500 or go to www.fsbbeaver.com**

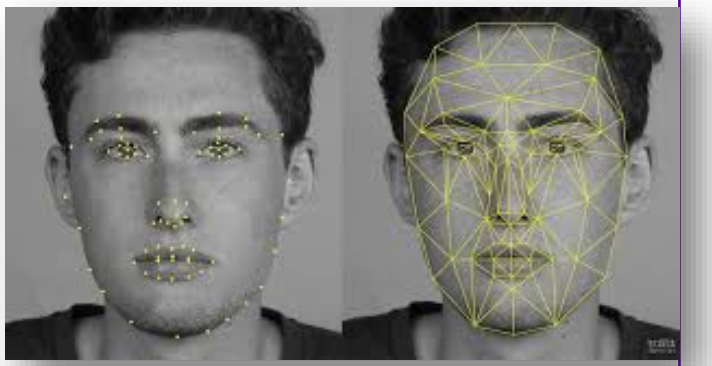
FCRA Information Sharing

Name: Fair Credit Reporting Act	1986
Applies to: Credit Reporting Agencies, generally and furnishers	1970
Summary: This law limits what may be included in a consumer report and to whom a consumer report may be furnished. CRAs must be diligent in reporting accurate information in all consumer reports and must investigate and remove all inaccurate information and information resulting from identity theft. Generally, an CRA may furnish a consumer report without authorization to a person that intends to use the information to determine credit worthiness for purposes such as • the extension of credit • employment determination • a business transaction imitated by the consumer.	Federal 15 USC § 1681 et seq.
Penalties: Up to $1,000 in civil damages, $2,500 in fines, and/or 2 years in prison.	
Enforcement: State AG, CFPB, and FTC, privacy suits	

FACTA Affiliate Marketing

Name: Fair and Accurate Credit Transactions Act	2003
Applies to: Entities possessing Eligibility Information	Federal
Summary: This law limits the use of Eligibility Information received from affiliates in the solicitation of products or services. • Any person intending to use a Eligibility Information received from an affiliate to solicit products or services must notify the consumer that the information will be used for such solicitation. • The consumer must have an opportunity to deny such information sharing and to chose to who and what type of information may be shared. • A prohibition of solicitations will last for 5 years. • Certain exceptions apply, including solicitation to persons who are engaged in a pre-existing relationship or to persons who initiated the solicitation. The FACT Act preempts state inconsistent with FCRA/FACTA.	Civil
Penalties: Civil	
Enforcement: Private parties, FTC, Regulatory Agencies	

Biometric Privacy Acts

Name: Various, but primary law is the Illinois Biometric Information Privacy Act (BIPA)	2008
Applies to: Private entities collecting or possessing Biometric Identifiers	State
Summary: BIPA: 1. Requires notice and consent for the collection of a Biometric Identifier or Biometric Information 2. Prohibits the sale of a Biometric Identifier or Biometric Information 3. Prohibits disclosure of a Biometric Identifier or Biometric Information without consent 4. Requires a written policy and retention schedule (with retention limits) for Biometric Identifiers or Biometric Information 5. Security around Biometric Identifiers or Biometric Information	Civil 
Penalties: Fines of up to the greater of $1,000 or actual damages/negligent violation, up to the greater of $5,000 or actual damages/intentional or reckless violation, plus attorneys' fees and costs	
Enforcement: Private right of action	

California Consumer Privacy Act (CaCPA)

Name: California Consumer Privacy Act	2018
Applies to: Entities doing business in California that collect personal information about state residents	California
Summary: The law expands several existing privacy rights for consumers and creates some new ones. The law gives state residents rights to: • Know personal information a business collects, the source of the information, the purposes for which the information is used and entities to which the information is shared • Demand deletion of personal information in some circumstances • Limit some information sharing with other entities • Not be treated differently if privacy rights are exercised Requirements will be clarified by rules to be issued by the Attorney General's Office	Civil
Penalties: Civil penalties up to $7,500/violation and statutory damages for certain security breaches	
Enforcement: California Attorney General	

General Data Protection Regulation (GDPR)

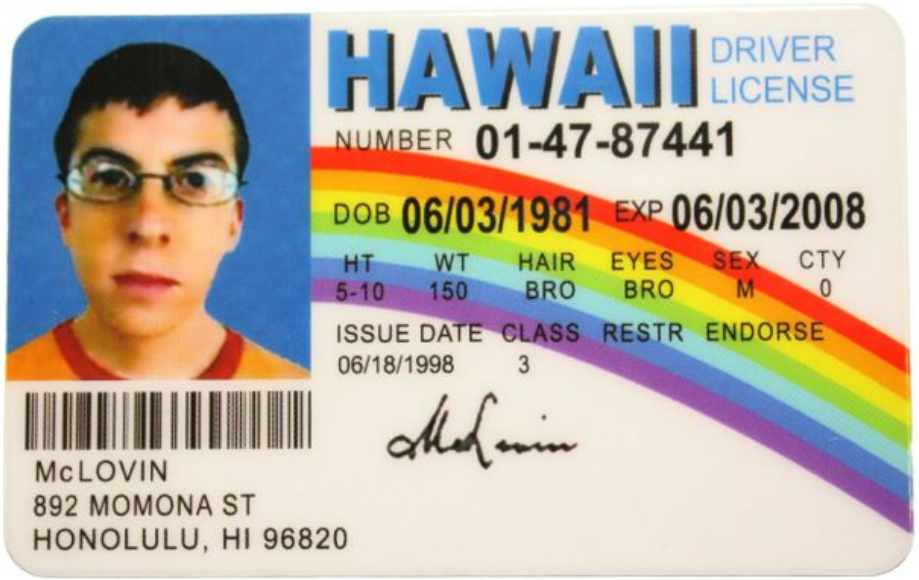
Name: General Data Protection Regulation	2018
Applies to: Entities established in the EU or targeting data subjects in the EU or monitoring their activity	EU
Summary: The GDPR expands and creates significant rights for Data Subjects including: • Right to be informed • Access to Personal Data • Rectification of Personal Data • Erasure (in some circumstances) • Restrict processing of Personal Data • Data portability • Objection to processing • Rights in relation to automated decision making and profiling	Civil
Penalties: Fines of up to the greater of 20 million Euros or up to 4% of the entity's global worldwide annual turnover for the prior year	
Enforcement: Data protection authorities	

HIPAA/HITECH Privacy

Name: Health Insurance Portability and Accountability Act & Health Information Technology for Economic and Clinical Health Act	1996 2009
Applies to: Covered Entities and, in some cases, Business Associates	Federal
The Privacy Rule limits how Covered Entities and Business Associates share and use Protected Health Information (PHI). PHI includes any payment history for healthcare, provision of healthcare, and past, present or future health conditions. (HIPAA)	Civil
Penalties: up to $50,000 in fines per violation with a $1,500,000 cap per year.	
Enforcement: HHS (OCR), FTC	

Driver's Privacy Protection Act (DPPA)

Name: Driver's Privacy Protection Act (DPPA)	1994
Applies to: State Department of Motor Vehicles and other authorized recipients of driver data	Federal 18 USC §2721
Summary: • Designed to protect privacy of personal information gathered by DMV; provides 14 specific purposes, unless further consent • Prohibits the release or use by any state of personal information with a motor vehicle record (govt., theft, fraud, insurance, court, DMV, tow, toll, etc.) • As of 2000, requires express opt-in from people before information is sold or released to 3rd party marketers • Many states have passed more stringent laws	Civil & Criminal
Penalties: $5,000 a day; civil violations	
Enforcement: State AG, DoJ, Civil penalties; Private Right of Action	



Video Privacy Protection Act (VPPA)

Name: Video Privacy Protection Act (VPPA)	1988
Applies to: Video Tape Service Provider	Federal 18 USC § 2710
Summary: • Meant to prevent the "wrongful disclosure of video tape rental or sale records [or similar audio visual materials, to cover items such as video games and the future DVD format]." • Passed the VPPA after Robert Bork's video rental history was published during his Supr • It makes any "video tape service provider" that discloses rental information outside th business liable for up to $2500 in actual damages. • 2013 - H.R. 6671, Obama approved an amendment that allows video rental companies consent to share information about their viewing preferences on social networks such	Civil & Criminal
Penalties: Criminal penalty, up to $5,000 in fines	
Enforcement: State AG, FTC	

Song-Beverly Act

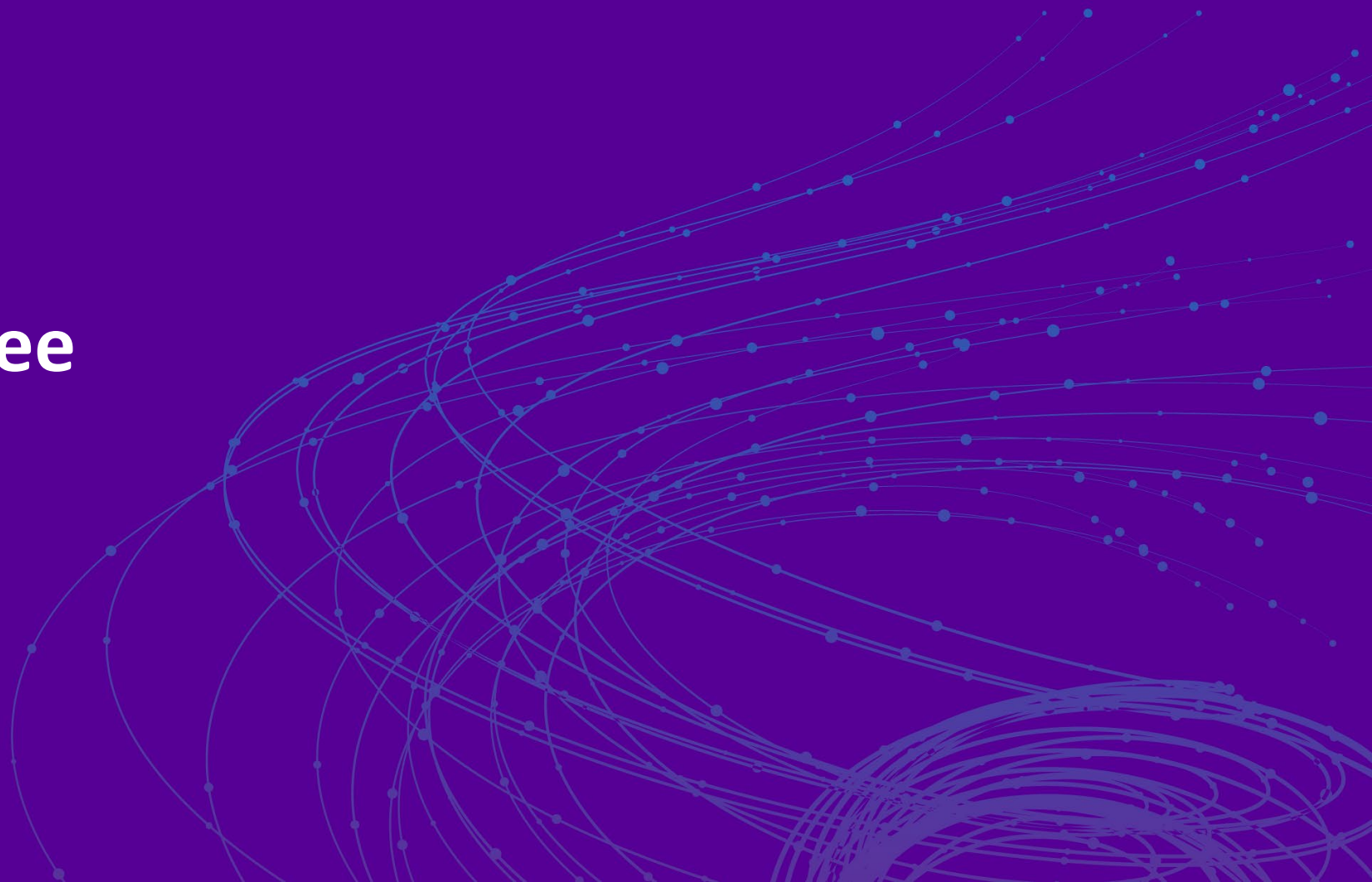
Name: Song-Beverly Credit Card Act of 1971	1971
Applies to: Persons accepting credit cards for the transaction of business	State Cal. Civ. Code § 1747.08
Summary: The law, among other things, prohibits a person accepting credit cards from requesting or requiring personal information to be put on the transaction form. Courts have found this to include address, telephone number and zip code.	Civil & Criminal
Penalties: Up to $250 for an initial violation and $1000 for subsequent violations	
Enforcement: AG and other state and local attorneys	

CAN-SPAM Act

Name: Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003	2003
Applies to: All US citizens, companies, or those with minimal contacts to the US	Federal 15 USC §§7701-7713
Summary: • Applies to "commercial electronic mail messages," which §3(2)(A) defines as electronic mail messages whose primary purpose is to advertise or promote a commercial product or service. • Pre-empts most state laws covering similar topic. • Criminal penalties – unauthorized access, retransmit spam, false headers, 5 or more accounts to send spam, false IP addresses and sends spam • Civil penalties for false/misleading information, false subject line, bad return address, opt-out in 10 days, physical address.	Civil & Criminal 
Penalties: 5 yrs. criminal penalty, $16,000 in fines per email; up to $2 million in parts	
Enforcement: State AG, FTC, DoJ, NO private right of action, ISPs	

RSAConference2019

Scenario Three



Scenario Three

- You are an app developer and are engaged to design and operate a mobile app for a bank
- The app will allow people to apply for a loan and sign in to manage the loan
- The app will collect personal information that will be sent to your servers then passed to the bank
- The bank wants users to be able to sign in using biometrics
- The bank operates in the US, but also serves Americans living abroad, like military families

Scenario Three

- Which privacy laws may apply to you
  - Directly?
  - Indirectly?
- What other privacy issues might you face?

RSAConference2019

Apply What You Have Learned

Apply in your business

This Month

- Review the list of laws (privacy & security) we have reviewed
- Determine which laws are most likely to impact you/your company
- Review the current projects you are engaged with to see if anything is being overlooked from a risk perspective

Apply in your business

Half Year

- Spend several hours each month reviewing the laws
- Use Wikipedia for each law that impacts your company/job
- Perform law firm website searches on these laws for PDFs detailing the latest changes/updates
- Try to put together an “Issue Spotting” list of those laws that might be triggered in your job/sector for easy reference

Apply in your business

By End of the Year

- Deeper dive those laws that you are using over and over again
- Create PPTs on the laws so you can better train your teams on what to look for in issue spotting exercises
- Determine which laws are changing rapidly and place Google News Updates on those specific phrases/laws
- Re-review this PPT for a refresher

RSAConference2019

Dr. Chris Pierson
CEO

BLACKCLOAK

chris@blackcloak.io

James T. Shreve
Partner

THOMPSON COBURN LLP

jshreve@thompsoncoburn.com